Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

SOBRE ANÉIS E MÓDULOS DISTRIBUTIVOS

Dissertação de Mestrado

RODRIGO DALLA VECCHIA

Porto Alegre , 25 de agosto de 2005

Dissertação submetida por Rdrig Dalla Vecchia [*], 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 (IMAT-UFRGS, ORIENTADOR)

Prof. Dr. Antônio Paques (IMAT-UFRGS)

Prof. Dr. Miguel Angel Alberto Ferrero (IMAT-UFRGS)

Prof. Dr. Plamen Emilov Kochloukov (IMAT-UFMG)

[*]Bolsista do CAPES

DEDICATÓRIA

Dedico esta dissertação aos meus pais e meu irmão que sempre deram o apoio necessário nas horas difíceis.

Agradecimentos

Agradeço à Fá, Léo, Sampaio, Bib's, por todo companheirismo. Ainda à Jonas, Dudu, Fábio, Ia, Cris, Chaninha, Rê, PC, Paulinho, Davi e a todo pessoal de Novo Hamburgo, em especial à Cissa, ao pessoal de Encantado, principalmente o do melhor time do mundo, Racing Futebol Arte, que são uma verdadeira família (...e agora Encantado, não tem mais a gente lá...), à Deivis, Jeanine, Rafa, Eve, Mana, Manão, Ritinha, Tila, Julinho, Anabel, Paulão, Douglas, Vani, Jéssica, Zé Bouviet, Zezinho, Joares, Célio, Lombriga, Crica (..."vamo acordá a Modesta"...), Sapo, Lila, à toda a família Magerl, à banda Megafônicos (Dani, Naso, Gu e Crica), Marquinhos, Seu Machado e esposa, Seu Ricardo (treinador) e esposa, Bélis e namorada (meu sócio do Béligão), Gustavo, Ique, Mancha, Marron, João, Sangalli, Tonini, Tim, Jones, Vaguinho, Ricardo, ao pessoal de Encantado que mora no 1403, à Gilton, Inês, à Samira, Mari, Gabizinha, Gabi, Aline, Renato e família Werle, Dudu (Ulbra), Aline Kruse, Maurício, Frasson, Elton e Michele.

Agradeço também aos meus mestres, dos quais destaco Giovanni Nunes (que foi meu orientador na graduação), Fabão, Cláudia, e Alveri Sant'Ana (meu atual orintador). A vocês agradeço não só por aprender matemática, mas por aprender para a vida. Gostaria também de citar Victor Coronel Aquino, Lica, Cydara e Jaime Ripoll e Eduardo.

Aos meus colegas, Ricardo, Edite, Diana, Tífane, Josué, Maurício, Bárbara, Edson e principalmente ao belo casal Lisiane e Elismar, que foram companheiros do início ao fim do curso e me ajudaram tanto nos momentos bons quanto nos momentos ruins.

À minha família pai, mãe, Fidêncio, Nanda, Tia Ode, Bibinha, Flávio, Jana, Gabi, Nelson, Nani, Lu (Peter), Rejane, vó Elsa, vó Olívia, Jane, e a todos da "turma da velinha"que invocavam todos os santos para uma ajudinha.

Enfim, agradeço a todos que de uma forma ou de outra contribuíram para esta grande conquista e peço desculpas se esqueci de citar alguém.

Resumo

Este trabalho tem por objetivo apresentar resultados sobre módulos e anéis distributivos. Trataremos de algumas caracterizações e propriedades desta classe de módulos. O teorema principal nos dá uma caracterização sobre módulos e anéis distributivos através de seus submódulos e ideais saturados.

Abstract

This work has for objective to present resulted on modules and distributive rings. We will deal with some characterizations and properties of this class of modules. The main theorem in gives to a characterization on modules and distributive rings through of its saturated submodules and ideals to them.

Índice

Introdução

Esta dissertação trata de anéis e módulos distributivos. Um módulo à direita M é chamado distributivo se, dados A, B e C submódulos de M, temos $(A + B) \cap C = (A \cap C) + (B \cap C)$. Dizemos que um anel R é distributivo à direita se o R-módulo à direita R_R é distributivo.

O primeiro trabalho importante sobre anéis e módulos distributivos foi publicado em em 1974, por Stephenson ([16]) e estas classes têm sido muito estudadas desde então. Em 1976, Brungs ([3]) mostrou que se R é um domínio ou um anel noetheriano à direita então R é distributivo à direita se, e somente se, R é localmente um anel de cadeia à direita (anel cujo reticulado de ideais à direita é linearmente ordenado por inclusão).

O resultado de Brungs pode facilmente ser generalizado para anéis onde o localizado em cada ideal maximal existe. Recentemente G. Puninski ([13]) e A. A. Tuganbaev ([18]) construíram exemplos de anéis distributivos não localizáveis, isto é, anéis em que o localizado em seus ideais maximais não existem. Em [7], M. Ferrero e A. Sant'Ana estudaram, entre outras coisas, o saturamento dos ideais à direita e obtiveram uma nova caracterização destes anéis, via ideais saturados, que permanece válida mesmo quando R não é um anel localizável.

O objetivo desta dissertação é estudar esta caracterização dada em [7].

Para tanto, começamos estudando anéis de cadeia e depois anéis e módulos distributivos à direita.

No capítulo 1, apresentaremos os pré-requisitos para a leitura desta dissertação.

No capítulo 2, trataremos sobre anéis de cadeia à direita, seguindo o estudo feito por C. Bessenrodt, H. H. Brungs e G. Törner [2]. Provaremos que todos os anéis desta classe são distributivos. O principal resultado será um teorema que nos permitirá analisar e construir ideais completamente primos em anéis de cadeia.

O capítulo 3 é baseado no artigo de W. Stephenson ([16]) que dá algumas caracterizações dos anéis e módulos distributivos à direita. Em particular, Stephenson mostra que M é um R-módulo à direita distributivo se, e somente se, para todo $x, y \in M$, temos $(xR : y) + (yR : x) = R$, onde $(xR : y) = \{a \in R \mid ya \in R\}$. Esta caracterização é fundamental para os cálculos feitos no que segue.

No capítulo 4, estudaremos as seções 2, 3 e 4 do trabalho de M. Ferrero e A. Sant'Ana ([7]). O principal resultado aqui, nos diz que um módulo sobre um anel admissível à direita é distributivo à direita se, e somente se, o reticulado dos submódulos S_P-saturados é linearmente ordenado por inclusão, onde $P \in Max(M)$.

Nesta dissertação consideraremos R um anel (com unidade) não necessariamente comutativo. O conjunto dos elementos inversíveis de R será denotado por $U(R)$ ou simplesmente U, quando não houver possibilidade de confusão com o anel base. Quando escrevermos $\subset$ ou $\supset$, estaremos considerando contenções estritas.

Capítulo 1

Pré-requisitos

Neste capítulo introduziremos a teoria básica para o desenvolvimento do trabalho que se segue.

1.1 Ideais Primos

Começamos definindo uma classe de ideais que embasará boa parte desta dissertação.

Definição 1.1. *Seja $P \neq R$ um ideal à direita do anel R.*

(i) P é chamado primo se, para ideais à direita A e B de R, temos que $AB \subseteq P$ implica $A \subseteq P$ ou $B \subseteq P$.

(ii) P é chamado semiprimo se, para todo ideal A de R tal que $A^2 \subseteq P$, temos $A \subseteq P$.

(iii) P é chamado completamente primo se, para $a, b \in R$, temos que $ab \in P$ implica $a \in P$ ou $b \in P$.

(iv) P é chamado completamente semiprimo se, para todo $a \in R$, temos

que $a^2 \in P$ implica $a \in P$.

(v) A intersecção de todos os ideais primos (bilaterais)de R é chamada de radical primo e denotado por $Rad(R)$.

As seguintes proposições estabelecem as equivalências mais usuais.

Proposição 1.2. *Seja P um ideal à direita de R, $P \neq R$. As seguintes condições são equivalentes:*

(i) P é um ideal primo de R.

(ii) Se $a, b \in R$ e $aRb \subseteq P$ então, $a \in P$ ou $b \in P$.

Demonstração:

$(i) \Rightarrow (ii)$ Sejam $a, b \in R$ tais que $aRb \subseteq P$. Então $aRbR \subseteq PR = P$. Como P é um ideal primo, temos $aR \subseteq P$ ou $bR \subseteq P$ e isto implica que $a \in P$ ou $b \in P$.

$(ii) \Rightarrow (i)$ Sejam A, B ideais à direita de R tais que $AB \subseteq P$. Se $A \nsubseteq P$, existe $a \in A$ tal que $a \in R \backslash P$. Logo, para cada $b \in B$ temos que $aRb \subseteq AB \subseteq P$ e assim $b \in P$. Conseqüentemente $B \subseteq P$ e a prova está completa. $\square$

Proposição 1.3. *Seja P um ideal à direita de R, $P \neq R$. As seguintes condições são equivalentes:*

(i) P é um ideal semiprimo de R.

(ii) Se $a \in R$ e $aRa \subseteq P$, então $a \in P$.

Demonstração:

$(i) \Rightarrow (ii)$ Seja $a \in R$ tal que $aRa \subseteq P$. Então $aRaR \subseteq PR = P$. Como P é um ideal semiprimo, temos $aR \subseteq P$ e isto implica que $a \in P$.

$(ii) \Rightarrow (i)$ Seja A um ideal à direita de R tal que $A^2 \subseteq P$. Observemos que para todo $a \in A$ temos $aRa \subseteq A^2 \subseteq P$ e isto implica que $a \in A$. Conseqüentemente $A \subseteq P$ e a prova está completa. $\square$

Um anel R é dito primo se (0) é um ideal primo de R. Usando a correspondência biunívoca entre ideais de R que contêm um ideal P e ideais de R/P, segue facilmente que P é um ideal primo de R se, e somente se, R/P é um anel primo.

O próximo lema será útil no capítulo 3 desta dissertação. Antes de enunciá-lo, faremos uma definição.

Definição 1.4. *Seja R um anel. Dizemos que $a \in R$ é um elemento nilpotente se existe $n \in \mathbb{N}$ satisfazendo $a^n = 0$. Dizemos que $a \in R$ é idempotente se $a^2 = a$.*

Lema 1.5. *Sejam R um anel e $e \in R$ um elemento idempotente. Então $R = eR \oplus (1-e)R$.*

Demonstração:

Trivialmente $R \supseteq eR + (1-e)R$. Para mostrar a outra contenção, basta notarmos que todo elemento $a \in R$ pode ser escrito da forma $a = ea + (1-e)a$. Com isso temos $R = eR + (1-e)R$. Resta verificar que a soma é direta. Para tanto, consideremos $x \in eR \cap (1-e)R$. Então $x = er_1$ e $x = (1-e)r_2$ para certos $r_1, r_2 \in R$. Segue que $er_1 = (1-e)r_2$. Multiplicando e à esquerda obtemos: $eer_1 = er_2 - eer_2$. Como e é idempotente vale: $er_1 = er_2 - er_2 = 0$ e isto implica que $x = 0$, uma vez que $x = er_1$. Pelo fato de $x \in eR \cap (1-e)R$ ser qualquer, obtemos $R = eR \oplus (1-e)R$. $\square$

1.2 Radical de Jacobson

Começaremos definindo o que será o objeto de estudo nesta seção.

Definição 1.6. *O Radical de Jacobson de um anel R, denotado por $J(R)$, é definido como a intersecção de todos os ideais maximais à direita de R.*

Lembremos que quando o anel tem unidade podemos mostrar, através do Lema de Zorn, que R sempre terá ideais maximais.

A seguir, provaremos um lema que nos dá uma caracterização dos elementos de $J(R)$ em termos dos elementos inversíveis à direita de R e em termos de um R-módulo simples à direita, que é definido abaixo.

Definição 1.7. *Sejam R um anel e M um R-módulo (à direita). M é um R-módulo simples se $M \neq 0$ e M não possui outros R-submódulos (à direita) além de (0) e M. Analogamente, um anel R é dito simples se $R \neq 0$ e se (0) e R são os únicos ideais de R.*

Lema 1.8. *Sejam R um anel e $y \in R$. Então as seguintes sentenças são equivalentes:*

(i) $y \in J(R)$.

(ii) $1 - yx$ é invertível à direita, para todo $x \in R$.

(iii) $My = 0$, para qualquer R-módulo simples à direita M de R.

Demonstração:

$(i) \Rightarrow (ii)$ Seja $y \in J(R)$. Se, para algum $x \in R$, $1 - yx$ não é invertível à direita, então $(1 - yx)R \neq R$ e está contido em algum ideal maximal à direita A de R. Mas $1 - yx \in A$ e $y \in A$, pois $y \in J(R)$, e isto implica que $1 \in A$, o que é uma contradição.

$(ii) \Rightarrow (iii)$ Suponhamos que $my \neq 0$, para algum $m \in M$. Então, como M é um R-módulo simples à direita, $myR = M$. Em particular, $m = myx$ para algum $x \in R$. Segue que $m(1 - yx) = 0$. Usando (ii) obtemos $m = 0$, o que é uma contradição.

$(iii) \Rightarrow (i)$ Para qualquer ideal maximal à direita A de R, R/A é um R-módulo simples à direita de R. Por (iii), $(R/A).y = 0$ implica que $y \in A$. Como A é qualquer ideal maximal à direita, temos, por definição, que $y \in J(R)$. $\square$

Definição 1.9. *O Radical de Jacobson de um R-módulo à direita M, denotado por $J(M)$, é definido como a interseccção de todos os submódulos maximais próprios de M. Se tais submódulos não existirem, então tomaremos $J(M) = M$.*

O seguinte lema nos será útil no capítulo 4.

Lema 1.10. *Sejam R um anel e M um R-módulo à direita. Então $MJ(R) \subseteq J(M)$, para todo módulo M.*

Demonstração:

Pelo lema anterior, $J(R)$ anula qualquer submódulo simples N. Então para todo homomorfismo $\varphi : M \longrightarrow N$, $\varphi(MJ(R)) = 0$. Observando que $J(M)$ pode também ser descrito por $J(M) = \{x \in M \mid \varphi(x) = 0$, *para todo* $\varphi : M \longrightarrow N$, *com* N *simples*$\}$ fica claro que $MJ(R) \subseteq J(M)$.

1.3 Anéis de Frações

Definição 1.11. *Sejam A um anel e S um subconjunto de A multiplicativamente fechado, isto é, $1 \in S$ e para todos $s, t \in S$ temos que $st \in S$. Definimos o anel de frações à direita de A com respeito a S como sendo o par (B, φ), onde B é um anel e $\varphi : A \longrightarrow B$ é um homomorfismo de anéis, chamado de aplicação canônica, satisfazendo as seguintes condições:*

F1. $\varphi(s)$ é invertível, para todo $s \in S$.

F2. Todo elemento em B tem a forma $\varphi(a)\varphi(s)^{-1}$, com $s \in S$.

F3. $\varphi(a) = 0$ *se, e somente se,* $as = 0$*, para algum* $s \in S$*.*

Proposição 1.12. *Seja S um subconjunto multiplicativamente fechado do anel A. Então o anel de frações B existe se, e somemte se, S satisfaz:*

S_1: Se $s \in S$ e $a \in A$, então existem $t \in S$ e $b \in A$ tais que $sb = at$.

S_2: Se $sa = 0$, com $s \in S$, então $at = 0$ para algum $t \in S$.

Além disso, quando B existe é da forma $B = (A \times S)/\sim$, onde $\sim$ é a relação de equivalência definida como $(a, s) \sim (b, t)$ se existem $c, d \in A$ tais que $ac = bd$ e $sc = td \in S$.

Demonstração:

Suponhamos que B existe e seja $\varphi : A \longrightarrow B$ a aplicação canônica. Primeiramente verificamos S_1. Seja $s \in S$ e $a \in A$. Então F2 nos dá $\varphi(s)^{-1}\varphi(a) = \varphi(b)\varphi(t)^{-1}$, para certos $b \in A$ e $t \in S$. Segue que $\varphi(a)\varphi(t) = \varphi(s)\varphi(b)$. Como φ é homomorfismo obtemos $\varphi(at) = \varphi(sb)$ e $\varphi(at - sb) = 0$. Por F3 temos que existe $u \in S$ tal que $atu = sbu$ e o resultado segue pois $tu \in S$ uma vez que S é multiplicativamente fechado. Para demonstrar S_2 consideremos $sa = 0$ com $s \in S$ e $a \in A$. Daí temos $\varphi(s)\varphi(a) = \varphi(sa) = \varphi(0) = 0$. Como $\varphi(s)$ é invertível obtemos $\varphi(a) = 0$. Agora, por F3, segue que $at = 0$ para algum $t \in S$. Portanto vale S_2.

Reciprocamente, suponhamos que S_1 e S_2 são satisfeitas. Tomando $(A \times S)/\sim$ definimos adição e multiplicação de maneira óbvia, isto é, dados $(a, s), (b, t) \in (A \times S)/\sim$ temos $(a, s) + (b, t) = (ac + bd, u)$, onde $u = sc = td \in S$ e $(a, s).(b, t) = (ac, tu)$ onde $sc = bu$ e $u \in S$. É fácil ver que a definição independe da escolha do representante da classe e $(A \times S)/\sim$ é um anel onde $(1, 1) = (s, s)$ é a unidade e $(0, s)$ é o zero do anel, para todo $s \in S$. Com isso definimos $\varphi : A \longrightarrow (A \times S)/\sim$ por $\varphi(a) = (a, 1)$, para todo $a \in A$. Obviamente φ está bem definida e é um homomorfismo. Mostremos agora, que φ definida dessa forma satisfaz F1, F2 e F3. Para verificar F1, consideremos $s \in S$. Segue que $\varphi(s) = (s,1)$. Afirmamos que $(1,s) = \varphi(s)^{-1}$. De fato $\varphi(s).(1,s) = (s,1).(1,s) = (sc, su)$ onde $1.c = 1.u$ e $u \in S$. Isto implica que $(sc, su) = (su, su) = (1,1)$ e a afirmação está provada. Como $s \in S$ é qualquer, $\varphi(s)$ é invertível para todo $s \in S$. Para verificar F2, mostraremos que dado $(a,s) \in (A \times S)/\sim$ temos $(a,s) = \varphi(a).\varphi(s)^{-1}$, o que é equivalente a dizer que $(a,s).\varphi(s) = \varphi(a)$, isto é, $(a,s).(s,1) = (a,1)$. Para tanto notemos que $(a,s).(s,1) = (ac, 1u)$ onde $sc = su$ e $u \in S$. Conseqüentemente $s(c-u) = 0$. Por S_2 existe $t' \in S$ tal que $(c-u)t' = 0$, isto é, $ct' = ut' \in S$. Segue que $(a,s).(s,1) = (ac, 1u) = (act', ut') = (act', ct') = (a,1)$. Para mostrar F3 basta observarmos que o elemento zero em $(A \times S)/\sim$ é da forma $(0,s)$ onde $s \in S$ é qualquer. Com isso obtemos $ker(\varphi) = \{a \in A \mid \exists s \in S$ *com* $as = 0\}$. $\square$

Proposição 1.13. *Quando $(A \times S)/\sim$ existe, possui a seguinte propriedade universal: para todo homomorfismo de anéis $\psi : A \longrightarrow C$ tal que $\psi(s)$ é invertível em C para todo $s \in S$ existe um único homomorfismo $\sigma : (A \times S)/\sim \longrightarrow C$ tal que $\sigma\varphi = \psi$, onde φ é a aplicação canônica.*

Demonstração:

Definimos $\sigma : (A \times S)/\sim \longrightarrow B$ por $\sigma(\varphi(a)\varphi(s)^{-1}) = \psi(a).\psi(s)^{-1}$ para todo $\varphi(a)\varphi(s)^{-1} \in (A \times S)/\sim$. Claramente σ está bem definida e é um homomorfismo. Começamos a demonstração mostrando que $\sigma\varphi = \psi$. Seja $a \in A$ então $(\sigma\varphi)(a) = \sigma((\varphi)(a)) = \sigma(\varphi(a)\varphi(1)^{-1}) = \psi(a)\psi(1)^{-1}$. Onde a segunda igualdade vale pois $\varphi(a) = \varphi(a.1) = \varphi(a).\varphi(1)$ e isto implica que $\varphi(a)\varphi(1)^{-1} = \varphi(a)$. Segue que $(\sigma\varphi)(a) = \psi(a)\psi(1)^{-1}$, isto é, $(\sigma\varphi)(a)\psi(1) = \psi(a)$. Observemos que $\psi(1) = 1$ pois ψ é homomorfismo, portanto $\psi(a) = (\sigma\varphi)(a).\psi(1) = (\sigma\varphi)(a).1 = (\sigma\varphi)(a)$. Para mostrar que σ é única, suponhamos que exista um homomorfismo τ tal que $\tau\varphi = \psi$. Seja $x \in (A \times S)/\sim$.

Pela propriedade F2, existe $a \in A$ e $s \in S$ tal que $x = \varphi(a)\varphi(s)^{-1}$. Segue que $\tau(x) = \tau(\varphi(a)\varphi(s)^{-1}) = \tau(\varphi(a)).\tau(\varphi(s)^{-1}) = \psi(a).\tau(\varphi(s)^{-1})$. Afirmamos que $\tau(\varphi(s)^{-1}) = \psi(s)^{-1}$. De fato, como τ é homomorfismo, vale $1 = \tau(1) = \tau(\varphi(s).\varphi(s)^{-1}) = \psi(s).\tau(\varphi(s)^{-1})$. Conseqüentemente $\tau(\varphi(s)^{-1}) = 1.\psi(s)^{-1} = \psi(s)^{-1}$. Assim temos $\tau(x) = \psi(a).\tau(\varphi(s)^{-1}) = \psi(a).(\psi(s)^{-1}) = \sigma(\varphi(a).\varphi(s)^{-1}) = \sigma(x)$, ou seja $\tau = \sigma$. □

Corolário 1.14. *Sejam ψ e σ definidas como na proposição anterior. Se ψ satisfaz F2 e F3, então σ é um isomorfismo.*

Demonstração:

Inicialmente vamos mostrar que $Ker(\sigma) = 0$. Seja $(a, s) \in Ker(\sigma)$. Então $0 = \sigma((a, s)) = \sigma(\varphi(a).\varphi(s)^{-1}) = \psi(a).\psi(s)^{-1}$. Segue que $\psi(a) = 0$, uma vez que $\psi(s)^{-1}$ é invertível. Por F3, existe $s' \in S$ tal que $s'a = 0$. Portanto $(a, s) = (s'a, s's) = (0, s's)$. Assim $Ker(\sigma) = 0$ e σ é injetiva. Consideremos agora $y \in B$. Por F2, $y = \psi(a).\psi(b)$ para certos $a \in A$ e $s \in S$. Com isso obtemos $y = \psi(a).\psi(s)^{-1} = (\sigma\varphi)(a).(\sigma\varphi)(s)^{-1} = \sigma(\varphi(a)\varphi(s)^{-1}) = \sigma((a, s).(1, s)) = \sigma((a, s))$. Portanto, basta tomarmos $(a, s) \in (A \times S)/\sim$ e temos $y = \sigma((a, s))$ verificando assim a sobrejetividade de σ. Logo σ é um isomorfismo. □

Para um anel de frações à direita (esquerda) de A com relação à S usaremos a notação $A[S^{-1}]$ ($[S^{-1}]A$), uma vez que são iguais, a menos de isomorfismos.

Usando o último corolário, obtemos o seguinte caso:

Corolário 1.15. *Se $A[S^{-1}]$ e $[S^{-1}]A$ existirem, então são isomorfos.*

Dizemos que S é um *conjunto de denominadores à direita* quando é multiplicativamente fechado e satisfaz S_1 e S_2. Além disso S é chamado *permutável* *à direita* se satisfaz S_1 e *reversível à direita* se satisfaz S_2. Dizemos também que um subconjunto $S \subseteq R$ multiplicativamente fechado é um *conjunto de Ore à direita* se S é permutável à direita, isto é, se dados $s \in S$ e $a \in R$ existirem $t \in S$ e $b \in R$ tais que $sb = at$.

Mostraremos que S_1 implica S_2 sob certas circunstâncias. Para tanto necessitamos da seguinte definição:

Definição 1.16. *Dado $S \subseteq A$, chamamos de anulador à direita de S ao conjunto $r(S) = \{a \in A \mid Sa = 0\}$.*

Observemos que $r(S)$ é um ideal à direita de A. Além disso, se $S = \{a\}$ então escrevemos $r(a)$ em lugar de $r(\{a\})$. Neste caso, $r(a)$ é dito um *anulador principal à direita.*

Proposição 1.17. *Consideremos que A satisfaz condições de cadeia ascendente para anuladores principais à direita. Se S é um conjunto multiplicativamente fechado de A e satisfaz S_1, então S é um conjunto de denominadores à direita.*

Demonstração:

Seja $sa = 0$ com $a \in A$ e $s \in S$. Devemos mostrar que existe $t \in S$ tal que $at = 0$. Pela condição de cadeia ascendente existe $n \in \mathbb{N}$ tal que $r(s^k) = r(s^n)$, para todo $k \geq n$. Por S_1 , existe $t \in S$ e $b \in A$ tal que $s^n b = at$. Então $s^{n+1}b = s(s^n b) = s(at) = (sa)t = 0$. Segue que $b \in r(s^{n+1}) = r(s^n)$. Portanto $at = s^n b = 0$. Logo S é um conjunto de denominadores à direita. $\square$

1.4 Módulos de Frações

Começamos definindo um módulo de frações.

Definição 1.18. *Sejam A um anel, M um A-módulo à direita e S um conjunto de denominadores à direita de A. Definimos o módulo de frações de*

M com respeito a S como sendo o $A[S^{-1}]$-módulo $M[S^{-1}] = (M \times S)/\sim$ onde $\sim$ é a relação de equivalência definida como $(x,s) \sim (y,t)$, se existem $c, d \in A$ tais que $xc = yd$ e $sc = td \in S$ com as operações dadas por:

$(x,s) + (y,t) = (xc + yd, u)$ onde $u = sc = td \in S$ (Usando S_1)

$(x,s).(b,t) = (xc, tu)$ para $(b,t) \in A[S^{-1}]$, onde $sc = bu$ e $u \in S$. □

Argumentando de modo semelhante à prova da Proposição 1.12 podemos mostrar que $M[S^{-1}]$, definido desta maneira, de fato é um $A[S^{-1}]$-módulo à direita.

Definição 1.19. *Sejam A um anel, M um A-módulo e $S \subseteq A$ um conjunto de denominadores à direita. Definimos:*

(a) $t(M) = \{x \in M \mid xs = 0$ para algum $s \in S\}$ o submódulo de S-torção.

(b) Se $M = t(M)$, então dizemos que M é um módulo de S-torção (Observemos que neste caso $M[S^{-1}] = 0$).

(c) Se $t(M) = 0$, então dizemos que M é um módulo livre de S-torção.

Definição 1.20. *Sejam A um anel, $S \subseteq A$ um conjunto de denominadores à direita e M um A-módulo à direita. Um submódulo L de M é dito S-saturado em M se satisfaz a seguinte propriedade: se $x \in M$ e $xs \in L$ para algum $s \in S$, então $x \in L$.*

Usaremos a notação $\mathcal{L}(M)$ para identificar o reticulado dos submódulos de um R-módulo M e notação análoga quando estivermos trabalhando apenas com ideais.

Proposição 1.21. *Sejam A um anel, $S \subseteq A$ um conjunto de denominadores à direita, M um A-módulo à direita e $\mu : M \longrightarrow M[S^{-1}]$, dada por $\mu(m) = (m, 1)$ (homomorfismo canônico), onde $m \in M$. Então:*

(i) Existe uma correspondência biunívoca entre submódulos S-saturados de M e $A[S^{-1}]$-submódulos de $M[S^{-1}]$.

(ii) M é um módulo livre de S-torção se, e somente se, $r(x)$ é S-saturado em A para todo $x \in M$.

(iii) Se A é um anel noetheriano à direita, então $A[S^{-1}]$ também o é.

Demonstração:

(i) Seja L um submódulo S-saturado de M. Consideremos a aplicação $\mu' : \mathcal{L}_{Sat}(A) \longrightarrow \mathcal{L}_{A[S^{-1}]}(M[S^{-1}])$ definida por $\mu'(L) = \mu(L) = L[S^{-1}]$. Vamos mostrar que através desta aplicação temos uma correspondência biunívoca entre submódulos S-saturados de M e $A[S^{-1}]$-submódulos de $M[S^{-1}]$. Para verificarmos a injetividade, consideremos K e L submódulos S-saturados tais que $K[S^{-1}] = L[S^{-1}]$ e provaremos que $K = L$. Para tanto, consideremos $x \in K$. Como $K[S^{-1}] = L[S^{-1}]$, existem $s, t \in S$ e $l \in L$ tais que $(x, s) = (l, t)$. Segue que $(x, s) - (l, t) = (0, 1)$. Pela propriedade da soma, $(xc - ld, u) = (0, 1)$ com $u = sc = td \in S$. Esta última igualdade equivale a dizer que existe $v \in S$ tal que $(xc - ld)v = 0$, isto é, $xcv = ldv$. Como L é submódulo temos que $ldv \in L$ e isto implica que $xcv \in L$. Pelo fato de S ser multiplicativamente fechado, $cv \in S$. Como L é S-saturado segue que $x \in L$. Assim, $K \subseteq L$. De maneira análoga, podemos provar a outra inclusão. Portanto μ' é injetiva. Vejamos agora a sobrejetividade. Seja N um $A[S^{-1}]$-submódulo de $M[S^{-1}]$. Devemos mostrar que $\mu^{-1}(N)$ é S-saturado. Para tanto, consideremos $x \in M$ tal que $xs \in \mu^{-1}(N)$ com $s \in S$. Se $xs \in \mu^{-1}(N)$, então $\mu(xs) = (xs, 1) = (x, t)$ para certo $t \in S$ pois $s \in S$. Conseqüentemente $x \in \mu^{-1}(N)$ e isto mostra que $\mu^{-1}(N)$ é S-saturado. Logo existe uma correspondência biunívoca entre os conjuntos dados.

(ii) Suponhamos que M é um módulo livre de S-torção. Então $t(M) = 0$, isto é, $xs = 0$, para algum $s \in S$, implica que $x = 0$. Sejam $a \in A$ e $s \in S$ tais que $as \in r(x)$. Então $xas = 0$. Como $s \in S$ temos, por hipótese, que $xa = 0$ e segue que $a \in r(x)$. Portanto $r(x)$ é S-saturado. Reciprocamente, suponhamos que $r(x)$ é S-saturado em A, para todo $x \in M$. Devemos mostrar que $t(M) = 0$. Para tal, consideremos $x \in M$ e $s \in S$ tais que $xs = 0$. Podemos escrever $x.1.s = 0$ e isto implica que $1.s \in r(x)$. Como $r(x)$ é S-saturado temos que $1 \in r(x)$, de onde segue que $x = 0$. Portanto M é um módulo livre de S-torção.

(iii) Consideremos $A_1 \subset A_2 \subset ... \subset A_n \subset ...$ uma cadeia ascendente de ideais à direita em $A[S^{-1}]$. Pelo ítem (i) desta proposição, existe uma bijeção entre os $A[S^{-1}]$-submódulos de $A[S^{-1}]$ e os ideais S-saturados de A dados pelo homomorfismo canônico μ. Então $\mu^{-1}(A_1) \subset \mu^{-1}(A_2) \subset ... \subset \mu^{-1}(A_n) \subset ...$ é uma cadeia de ideais à direita S-saturados em A. Como A é noetheriano, esta cadeia é estacionária. Segue através da bijeção que a cadeia $A_1 \subset A_2 \subset ... \subset A_n \subset ...$ é estacionária também. Logo $A[S^{-1}]$ é noetheriano à direita. $\square$

1.5 Aritmética de Ideais

Nesta seção falaremos sobre alguns aspectos úteis sobre ideais de um anel.

Começamos definindo anéis distributivos:

Definição 1.22. *Seja R um anel. Então R é um anel distributivo se para quaisquer ideais A, B, $C \subseteq R$ temos:*

(i) $A \cap (B + C) = (A \cap B) + (A \cap C)$ ou equivalentemente

(ii) $A + (B \cap C) = (A + B) \cap (A + C)$.

Notemos que a contenção $A \cap (B + C) \supseteq (A \cap B) + (A \cap C)$ (ou equivalentemente $A + (B \cap C) \subseteq (A + B) \cap (A + C)$) sempre é válida.

Observemos também que esta definição pode ser estendida a módulos, como veremos no início do capítulo 3.

Consideremos agora a seguinte versão do Teorema Chinês dos Restos:

Teorema Chinês dos Restos: Sejam R um anel com unidade, $I_1, I_2, ..., I_n$ ideais de R e $a_1, a_2, ..., a_n \in R$ tais que $a_i \equiv a_j (mod\ I_i + I_j)$, com $i, j = 1, 2, ..., n$. Então o sistema de congruências $x \equiv a_1 (mod\ I_1)$, $x \equiv a_2 (mod\ I_2)$, ..., $x \equiv a_n (mod\ I_n)$ tem solução em R.

Os próximos resultados mostram uma equivalência entre distributividade e o Teorema Chinês dos Restos.

Proposição 1.23. *Seja R um anel onde o Teorema Chinês dos Restos é válido. Então R é um anel distributivo.*

Demonstração:

Sejam I, J, K ideais de R. Vamos mostrar que $(I + J) \cap (I + K) \subseteq I + (J \cap K)$, uma vez que a outra contenção sempre é válida. Para tanto, consideremos $a \in R$, tal que $a \in (I + J) \cap (I + K)$. Então $a \equiv 0 (mod\ I + J)$, $a \equiv 0 (mod\ I + K)$ e $a \equiv a (mod\ J + K)$. Como o Teorema Chinês dos Restos é válido, o sistema $x \equiv 0 (mod\ I)$, $x \equiv a (mod\ J)$ e $x \equiv a (mod\ K)$ tem solução. Assim, existe $x \in R$ tal que $x \in I$ e $x - a \in J \cap K$. Tomando $y = a - x \in J \cap K$, obtemos $a = x + y \in I + (J \cap K)$. Portanto vale a inclusão acima. Logo R é distributivo. $\square$

O próximo resultado nos fornece a recíproca da proposição acima.

Proposição 1.24. *Seja R um anel distributivo. Então vale o Teorema Chinês dos Restos.*

Demonstração:

Usaremos o método indutivo para demonstrar esta proposição. Para tanto, consideremos I_1, I_2 ideais de R e $a_1, a_2 \in R$ tais que $a_1 \equiv a_2(mod\ I_1 + I_2)$. Vamos mostrar que o sistema de congruências $x \equiv a_1(mod\ I_1)$ e $x \equiv a_2(mod\ I_2)$ tem solução em R. Como $a_1 \equiv a_2(mod\ I_1 + I_2)$, existem $e_1 \in I_1$ e $e_2 \in I_2$ tais que $a_1 - a_2 = e_1 + e_2 \in I_1 + I_2$. Logo, para solucionarmos o sistema, basta tomarmos $x = a_1 - e_1 = a_2 + e_2$. Suponhamos que o sistema de congruências vale para certo $n-1 \in \mathbb{N}$, isto é, $x \equiv a_1(mod\ I_1)$, $x \equiv a_2(mod\ I_2)$, ..., $x \equiv a_{n-1}(mod\ I_{n-1})$ tem pelo menos uma solução $y \in R$, onde $I_1, I_2, ..., I_{n-1}$ são ideais de R e $a_1, a_2, ..., a_{n-1} \in R$ são tais que $a_i \equiv a_j(mod\ I_i + I_j)$, com $i, j = 1, 2, ..., n-1$ e mostraremos que também é válido para $n \in \mathbb{N}$. Consideremos agora o sistema: $x \equiv y(mod\ \bigcap_{i=1}^{n-1} I_i)$ e $x \equiv a_n(mod\ I_n)$. Então, para $1 \leq i \leq n-1$ temos, $y - a_n = y - a_i + a_i - a_n \in I_i + (I_i + I_n) = I_i + I_n$. Conseqüentemente $y \equiv a_n(mod\ \bigcap_{i=1}^{n-1}(I_i + I_n))$. Como R é um anel distributivo, obtemos $\bigcap_{i=1}^{n-1}(I_i + I_n)) = (\bigcap_{i=1}^{n-1} I_i) + I_n$. Pelo caso $n = 2$, existe $z \in R$ que satisfaz o último sistema de congruências. Assim, segue de $z \equiv y(mod\ \bigcap_{i=1}^{n-1} I_i)$ que $z - y \in \bigcap_{i=1}^{n-1} I_i$, isto é, $z - y \in I_i$ para todo $i = 1, 2, ..., n-1$. Temos ainda, da hipótese de indução, que $y - a_i \in I_i$ para todo $i = 1, 2, ..., n-1$. Daí, $(z - y) + (y - a_i) = z - a_i \in I_i$, uma vez que $(z - y)$ e $(y - a_i)$ pertencem a I_i, com $i = 1, 2, ..., n-1$. Portanto $z \equiv a_i(mod\ I_i)$ para $i = 1, 2, ..., n$ e o teorema está mostrado. $\square$

Com as duas proposições anteriores temos que um anel R é distributivo se, e somente se, vale o Teorema Chinês dos Restos.

Exemplo 1.25. O anel $\mathbb{Z}$ é um anel distributivo pois, como o Teorema Chinês dos Restos é válido, o resultado fica imediato pelas proposições 1.23 e 1.24. $\square$

Capítulo 2

Anéis de Cadeia à Direita

Neste capítulo , após introduzir algumas notações e definições, trataremos de fatos elementares sobre ideais à direita em anéis de cadeia à direita. Aqui, seguiremos o trabalho de C. Bessenrodt, H. H. Brungs e G. Türner ([2]).

2.1 Terminologia e Notações

Começaremos introduzindo a definição de anés de cadeia.

Definição 2.1. *Um anel R é chamado anel de cadeia à direita (esquerda) se $aR \subseteq bR$ ou $bR \subseteq aR$ ($Ra \subseteq Rb$ ou $Rb \subseteq Ra$), para quaisquer elementos $a, b \in R$. Se R é um anel de cadeia à direita e à esquerda ao mesmo tempo, então R será chamado um anel de cadeia.*

Segue imediatamente da definição que anéis de cadeia à direita são locais, isto é, possuem exatamente um ideal maximal à direita, que é exatamente o radical de Jacobson denotado por $J(R)$. Neste caso, trivialmente, $J(R)$ é um ideal bilateral de R consistindo no conjunto dos elementos não invertíveis de

R.

Abaixo vemos um exemplo de anel de cadeia.

Exemplo 2.2. Os ideais de $\mathbb{Z}_8$ são , $<\overline{0}>=\{\overline{0}\}$, $<\overline{2}>=<\overline{6}>=\{\overline{0},\overline{2},\overline{4},\overline{6}\}$, $<\overline{4}>=\{\overline{0},\overline{4},\}$ e $<\overline{1}>=<\overline{3}>=<\overline{5}>=<\overline{7}>=\mathbb{Z}_8$, o que nos leva a concluir que $\mathbb{Z}_8$ é um anel de cadeia. $\square$

O próximo lema é uma lista de observações iniciais. Para demonstrá-lo necessitaremos ainda da definição abaixo.

Definição 2.3. *Seja R um anel de cadeia e A, B ideais à direita de R tais que $A \supset B$. Dizemos que A e B são vizinhos se, $A \supseteq C \supseteq B$, para um ideal à direita C, implicar $A = C$ ou $B = C$. Denotemos isto por $A \succ B$ ou $B \prec A$. Se incluirmos a igualdade usaremos $A \succeq B$ ou $B \preceq A$.*

Lema 2.4. *Seja R um anel de cadeia à direita. Então as sentenças abaixo são verdadeiras:*

(i) Os ideais à direita de R são linearmente ordenados por inclusão.

(ii) Todos os ideais à direita finitamente gerados são ideais principais à direita.

(iii) Se R é um domínio, então quaisquer dois ideais principais à esquerda com intersecção diferente de zero são comparáveis.

(iv) Se R é um domínio com a propriedade de que a intersecção de dois quaisquer ideais principais é diferente de (0), então R é um domínio de cadeia.

(v) Sejam A e B ideais à direita, com $A \succ B$, então $A = aR$ e $B = aJ(R)$ para algum $a \neq 0$ em R.

Demonstração:

(i) Para demonstrar (i) consideremos A e B ideais à direita de R . Suponhamos que $A \nsubseteq B$. Então existe $a \in A$ tal que $a \notin B$. Como R é um anel de cadeia, segue que, para todo $x \in B$, $x \in aR$. Portanto $B \subseteq aR \subseteq A$.

(ii) Seja I um ideal à direita finitamente gerado de R, isto é, $I = \langle b_1, b_2, ..., b_n \rangle$, para certos $b_1, b_2, ..., b_n \in R$. Como R é anel de cadeia, temos que $b_iR \subseteq b_jR$ ou $b_jR \subseteq b_iR$, para quaisquer $i, j \in \{1, 2, ..., n\}$. Por (i) garantimos que existe b_i tal que $b_iR \supseteq b_jR$ para todo $j \in \{1, 2, ..., n\}$. Segue que $I \subseteq b_iR$. Logo $I = b_iR$.

(iii) Consideremos Ra e Rb dois ideais à esquerda tais que $Ra \cap Rb \neq 0$. Então $r_1a = r_2b \neq 0$ para certos $r_1, r_2 \in R$. Como R é anel de cadeia à direita, podemos assumir $r_1t = r_2$, com $t \in R$. Conseqüentemente $r_1a = r_2b = r_1tb$, donde segue que $r_1(a - tb) = 0$, ou seja, $a = tb$, pois R é um domínio. Logo $Ra \subseteq Rb$.

(iv) Segue direto de (iii).

(v) Sejam A e B ideais à direita de R com $A \succ B$. Consideremos $a \in A \backslash B$. Consideremos ainda $J(R)$ o radical de Jacobson do anel R. Como R é anel de cadeia temos que R é local e isto implica que $J(R) \prec R$. Segue que $aJ(R) \prec aR \subseteq A$. Mostremos agora que $B \subseteq aJ(R)$. Se, por absurdo, $aJ(R) \subseteq B$, com $aJ(R) \neq B$, teríamos que existe $b \in B$ tal que $b = ar$, para algum $r \in R$, com r invertível. Daí $br^{-1} = a$ e então $a \in B$, o que é um absurdo. Portanto $B \subseteq aJ(R) \prec aR \subseteq A$ e usando a hipótese de que A e B são vizinhos concluímos $A = aR$ e $B = aJ(R)$. $\square$

Abaixo definiremos algumas noções que nos serão úteis para a proposição que se segue.

Definição 2.5. *Um anel R é dito de Bezout à direita (esquerda) se para dois quaisquer ideais principais à direita (esquerda) , sua soma e sua intersecção* *são também ideais principais à direita (esquerda).*

Recordamos a Definição 1.22 que diz que um anel R é distributivo à direita se $A\cap(B+C) = (A\cap B)+(A\cap C)$, para quaisquer ideais à direita A, B, $C \subseteq R$.

Sabemos, do Exemplo 1.25, que $\mathbb{Z}$ é um anel distributivo. Facilmente vemos que, dados dois ideais $a\mathbb{Z}$ e $b\mathbb{Z}$ de $\mathbb{Z}$ ($\mathbb{Z}$ é um domínio de ideais principais), $a\mathbb{Z}+b\mathbb{Z} = mdc(a,b)\mathbb{Z}$ e $a\mathbb{Z}\cap b\mathbb{Z} = mmc(a,b)\mathbb{Z}$. Portanto, $\mathbb{Z}$ é um domínio de Bezout, mas não é um anel de cadeia, uma vez que, se $p,q \in \mathbb{Z}$ são primos, $p\mathbb{Z} \nsubseteq q\mathbb{Z}$ e $q\mathbb{Z} \nsubseteq p\mathbb{Z}$.

O próximo exemplo mostra que a classe de anéis de Bezout e a classe de anéis distributivos não coincidem.

Exemplo 2.6. Considere o anel $R = \mathbb{Z}[\sqrt{-5}]$. Então R é um domínio de Dedekind e portanto vale o Teorema Chinês dos Restos ([5]). Logo pela proposição 1.23, R é distributivo. Agora, o ideal $I =< 2, 1+\sqrt{-5} >= 2R+(1+\sqrt{-5})R$ não é principal ([11]). Logo R é um anel distributivo, mas não é um anel de Bezout. $\square$

Proposição 2.7. *Para um anel R as seguintes sentenças são equivalentes:*

(a) *R é um anel de cadeia à direita.*

(b) *R é um anel local de Bezout à direita.*

(c) *R é um anel local distributivo à direita.*

Demonstração:

(a) $\Rightarrow$ (b) Sejam aR e bR ideais principais de R. Como R é um anel de cadeia à direita, R é local e $aR \subseteq bR$ ou $bR \subseteq aR$. Sem perda de generalidade, suponhamos $aR \subseteq bR$. Segue que $aR + bR = bR$ e $aR \cap bR = aR$. Portanto, R é um anel local de Bezout à direita.

$(a) \Rightarrow (c)$ Pelo Lema 2.4 os ideais do anel R são linearmente ordenados por inclusão, o que torna a demonstração trivial.

$(b) \Rightarrow (a)$ Sejam $0 \neq a, b \in J(R)$. Como R é um anel local de Bezout à direita, existe $c \in R$ tal que $aR + bR = cR$, com $aR, bR \subseteq cR$. Se a e b estão ambos em $cJ(R)$, então $cR = cJ(R)$ e daí teríamos $c = 0$, o que é um absurdo. Sem perda de generalidade, suponhamos que $a \notin cJ(R)$. Como $aR \subseteq cR$ temos $a \in cR$. Então podemos escrever $a = cr$, com $r \notin J(R)$, o que implica que r é invertível à direita. Segue que $ar^{-1} = c$ e concluímos que $cR \subseteq aR$. Daí $cR = aR$ e portanto $bR \subseteq cR = aR$.

$(c) \Rightarrow (a)$ Sejam $a, b \in R$. Daí temos $aR = aR \cap (bR + (a-b)R) = (aR \cap bR) + (aR \cap (a-b)R)$. Como $a \in aR$ temos $a = r + (a-b)t$, onde $r \in aR \cap bR$ e $t \in R$. Segue que $a = r + at - bt$, ou seja, $a - at = r - bt$ e conseqüentemente $a(1-t) = r - bt$. Com isso temos $a(1-t) \in bR$ e $bt \in aR$. Se $t \notin J(R)$, então t é invertível à direita. Como $bt \in aR$ obtemos $bt = ar$, ou seja, $b = art^{-1}$. Segue que $bR \subseteq aR$. Se $t \in J(R)$, então $1 - t$ é invertível à direita. Daí temos $a(1-t) = br_2$, ou equivalentemente, $a = br_2(1-t)^{-1}$, com $r_2 \in R$, e isto implica que $aR \subseteq bR$. Portanto R é um anel de cadeia à direita. □

2.2 Ideais à direita em anéis de cadeia à direita.

Nesta seção mostraremos alguns resultados básicos sobre ideais à direita em anéis de cadeia à direita. O lema seguinte nos mostra que um ideal à direita $I \subseteq R$ é um ideal à esquerda se $UI = I$.

Lema 2.8. *Seja R um anel de cadeia à direita e $a \in R$. Então $Ra \subseteq UaR$, onde U é o conjunto dos elementos inversíveis de R.*

Demonstração: Seja $x \in R$. Se $x \in U$, então $xa = xa1 \in UaR$. Se $x \notin U$, consideramos os ideais aR e xaR. Como R é anel de cadeia à direita, temos $xaR \subseteq aR$ ou $aR \subseteq xaR$. No primeiro caso $xa = ar = 1ar \in UaR$ para algum $r \in R$. No segundo caso existe $s \in R$ tal que $xas = a$. Se $s \notin J(R)$, s seria invertível e teríamos $xa \in aR$, que já foi analisado no primeiro caso. Se $s \in J(R)$ então $1 + s \in U$ donde obteríamos $(x + 1)a = xa + a = xa + xas = xa(1 + s)$, ou seja, $xa = (x + 1)a(1 + s)^{-1} \in UaR$, uma vez que $1 + x \in U$, já que $x \notin U$ □

O próximo lema é uma lista de alguns fatos gerais sobre ideais à direita em anéis de cadeia.

Lema 2.9. *Seja R um anel de cadeia à direita.*

(i) Seja A um ideal à direita do semigrupo multiplicativo do anel R. Então A também é um ideal à direita de R.

(ii) Um subgrupo aditivo A de R é um ideal à direita se $Au \subseteq A$, para todo $u \in U$.

(iii) Um ideal à direita A de R é um ideal bilateral se $uA \subseteq A$, para todo $u \in U$.

(iv) Sejam A um ideal à direita de R e B um ideal bilateral de R. Então

$$A.B = \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in A, b_i \in B\} = \{ab \mid a \in A, b \in B\}.$$

Demonstração:

(i) É suficiente provar que A é grupo aditivo do anel R. Seja $a, b \in A$. Como R é anel de cadeia, podemos supor, sem perda de generalidade, que $ar = b$, para algum $r \in R$. Então $a - b = a(1 - r) \in A$, pois A é um ideal à direita do semigrupo multiplicativo do anel R.

(ii) Seja $b \in A$ e $r \in R$. Se $r \in U$, então $br \in A$ e não há o que mostrar. Em caso contrário, $r \in J(R)$ e isto equivale a dizer que $1 + r \in U$. Segue que $b(1+r) \in A$, isto é, $b+br \in A$. Como $b \in A$ e A é um subgrupo aditivo temos que $br \in A$. Logo A é um ideal à direita.

(iii) Seja $b \in A$. Pelo Lema 2.8 $Rb \subseteq UbR \subseteq UA \subseteq A$, onde a segunda contenção é válida pois $b \in A$ e A é ideal à direita. Portanto A é ideal à esquerda, logo, bilateral.

(iv) Obviamente $\{ab|\ a \in A, b \in B\}$ está contido em $A.B$. Seja $\sum_{i=1}^{n} a_i b_i \in A.B$. Como R é anel de cadeia à direita, suponhamos, sem perda de generalidade, que $a_1R \supseteq a_iR$ e $a_1r_i = a_i$ para todo $i \in \{1,2,...,n\}$. Então $\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} a_1 r_i b_i = a_1 \sum_{i=1}^{n} r_i b_i \in \{ab \mid a \in A, b \in B\}$, pois $\sum_{i=1}^{n} r_i b_i \in B$, uma vez que $b_i \in B$ e B é ideal bilateral. $\square$

Definição 2.10. *Seja I um ideal de um anel R. Dizemos que I é nil se todos os elementos de I são nilpotentes, isto é, para cada $a \in I$ existe $n \in \mathbb{N}$ satisfazendo $a^n = 0$.*

Como conseqüência do Lema 2.9, obtemos o seguinte resultado:

Lema 2.11. *Seja I um ideal à direita de um anel de cadeia à direita R. Então:*

(i) $\overline{I} = \bigcup_{u \in U} uI$ é o menor ideal bilateral contendo I e $\underline{I} = \bigcap_{u \in U} uI$ é o maior ideal bilateral contido em I.

(ii) $\overline{I}$ é nil se, e somente se, o ideal à direita I é nil.

Demonstração:

(i) Para demonstrar que $\overline{I}$ possui todas as características acima citadas, mostraremos inicialmente que $RI = \bigcup_{u \in U} uI = \overline{I}$. De fato, pelo Lema 2.8 temos $RI \subseteq UIR \subseteq UI \subseteq \bigcup_{u \in U} uI \subseteq RI$. Segue que $\overline{I}$ é um ideal de R pois I é ideal á direita. Além disso, $u\overline{I} \subseteq \overline{I}$, para todo $u \in U$. Portanto, pelo Lema 2.9(iii) temos que $\overline{I}$ é um ideal bilateral. Para completar a demonstração resta apenas a minimalidade. Para tanto, consideremos B o menor ideal bilateral que contém I. Então, como o anel R é de cadeia à direita, vale $B \subseteq \overline{I} = RI$. Suponhamos, por absurdo, que existe $a \in RI$ tal que $a \notin B$. Mas $a = ui$ para algum $u \in U$ e algum $i \in I$. Isto implica que $u^{-1}a = i$, istó é, $u^{-1}a \in I \subseteq B$. Como B é ideal bilateral, $a = uu^{-1}a \in B$, o que é um absurdo. Segue que $B = \overline{I}$. Assim provamos o primeiro ítem do lema. Analogamente obtemos que $\underline{I} = \bigcap_{u \in U} uI$ é o maior ideal bilateral contido em I.

(ii) Suponhamos que $\overline{I}$ é nil. Como $I \subseteq \overline{I}$ temos que para todo $i \in I$ existe $n \in \mathbb{N}$ tal que $i^n = 0$. Reciprocamente suponhamos que I é nil. Seja $x \in \overline{I}$. Então $x = ai$, para certos $a \in R$ e $i \in I$. Observemos que $ia \in I$, uma vez que I é ideal à direita de R. Portanto, existe $m \in \mathbb{N}$, tal que $(ia)^m = 0$. Segue que $(ai)^{m+1} = a(ia)^m i = 0$. Como $x \in \overline{I}$ é arbritário, temos que $\overline{I}$ é nil. $\square$

Uma das versões da conjectura de Koethe afirma que um nil ideal unilateral está sempre contido em um nil ideal bilateral. O resultado acima mostra que não existe contra-exemplo para esta conjectura na classe dos anéis de cadeia.

Falaremos agora sobre um dos instrumentos principais deste capítulo, que são os ideais primos.

O próximo resultado mostra que, em anéis de cadeia à direita, ideais primos e semiprimos coicidem. Além disso, um ideal bilateral completamente semiprimo é na verdade ideal completamente primo nesta classe de anéis.

Lema 2.12. *Seja R um anel de cadeia à direita e P um ideal à direita de R. Então:*

(i) P é primo se, e somente se, $xRx \subseteq P$ implica $x \in P$.

$(ii)P$ é primo se e somente se $X^2 \subseteq P$ implica $X \subseteq P$ para todo ideal à direita X.

(iii) Consideremos P um ideal bilateral de R. P é um ideal completamente primo se, e somente se, $x^2 \in P$ implica que $x \in P$.

Demonstração:

(i) Suponhamos que que P é primo, então, pela Proposição 1.2, $xRx \subseteq P$ implica que $x \in P$. Reciprocamente suponhamos que $xRx \subseteq P$ implica $x \in P$ e consideremos $x, y \in R$ tal que $xRy \subseteq P$. Como R é um anel de cadeia à direita, existem dois casos a serem analisados: $xR \subseteq yR$ ou $yR \subseteq xR$. No primeiro caso temos $xRxR = xR(xR) \subseteq xRyR = (xRy)R \subseteq P$. Em particular obtemos $xRx \subseteq P$ e por hipótese $x \in P$. No segundo caso, o resultado segue analogamente. Portanto P é primo.

(ii) O resultado segue diretamente da Definição 1.1(ii), da Proposição 1.3 e do ítem (i) deste Lema.

(iii) Se P é um ideal completamente primo de R e $x^2 \in P$ então claramente $x \in P$. Por outro lado, suponhamos que $x^2 \in P$ implica que $x \in P$ e sejam $x, y \in R$ tais que $xy \in P$. Como R é anel de cadeia, temos que $x = ys_1$ ou $y = xs_2$, para certos $s_1, s_2 \in R$. No primeiro caso $x^2 = xys_1 \in P$, pois $xy \in P$. Segue disso que $x \in P$. No segundo caso, notemos que $y(xy)x \in P$, pois P é bilateral. Então $(yx)^2 \in P$ o que implica que $yx \in P$. Daí, $y^2 = yxs_2 \in P$ e conseqüentemente $y \in P$. $\square$

Lema 2.13. *Seja R um anel de cadeia à direita e $A \neq R$ um ideal unilateral de R com $R \backslash A$ multiplicativamente fechado. Então A é um ideal bilateral completamente primo.*

Demonstração:

Consideremos inicialmente o caso em que A é ideal à direita de R. Para demonstrar que A é bilateral afirmamos que $uA \subseteq A$, para todo $u \in U$. Seguirá daí que A é bilateral pelo Lema 2.9(iii). De fato, seja $u \in U$. Suponhamos, por absurdo, que $uA \nsubseteq A$. Então, para algum $a \in A$, temos $ua \in R \backslash A$. Notemos que nenhum invertível pode pertencer a A pois $A \neq R$. Como $R \backslash A$ é multiplicativamente fechado, $u^{-1}.ua \in R \backslash A$ o que implica que $a \in R \backslash A$ e isto é um absurdo. Portanto $uA \subseteq A$. Para o caso em que A é ideal à esquerda basta verificarmos que $Au \subseteq A$, para todo $u \in U$, cuja demonstração é análoga a acima. Agora, usando o Lema 2.9(ii) é imediato que A é bilateral. Resta provar que A é completamente primo. Para tanto, suponhamos que $xy \in A$, com $x \notin A$. Conseqüentemente $y \in A$ pois caso contrário teríamos que $xy \notin A$ devido ao fato de $R \backslash A$ ser multiplicativamente fechado. $\square$

Observemos que na última parte da demonstração não utilizamos o fato de R ser um anel de cadeia. Portanto, se R é um anel e A é um ideal unilateral tal que $R \backslash A$ é multiplicamente fechado, então A é completamente primo.

Além disso, se A é um ideal unilateral completamente primo, então claramente $R \backslash A$ é multiplicativamente fechado.

Esta última informação, aliada ao Lema 2.13 nos garante que, em um anel de cadeia à direita R, todo ideal à direita completamente primo de R é bilateral.

Podemos agora demonstrar o seguinte lema que, apesar de ser simples, é muito útil para o que segue.

Lema 2.14. *Sejam R um anel de cadeia à direita e P um ideal completamente primo de R. Então $P = sP$, para todo $s \notin P$.*

Demonstração:

Consideremos $s \notin P$. Como R é anel de cadeia, $P \subseteq sR$ e isto implica que para todo $p \in P$ existe $x \in R$ tal que $p = sx$. De P completamente primo segue que $x \in P$, donde temos $P \subseteq sP$. A outra inclusão é clara, uma vez que P é um ideal bilateral. $\square$

2.3 Saturamento de ideais à direita e ideais primos

Vamos definir alguns conjuntos e ideais associados com um dado ideal à direita. Em nosso estudo, R será um anel de cadeia à direita e I um ideal à direita de R.

Para $s \in R$, consideremos o seguinte conjunto:

$$Is^{-1} = \{x \in R \mid xs \in I\}.$$

Este conjunto contém I e é fechado perante à adição, mas, em geral, não é um ideal à direita de R. Obviamente, se I é um ideal bilateral, então Is^{-1} é um ideal à esquerda. Abaixo construiremos um ideal à direita associado ao ideal à direita I.

Lema 2.15. *Sejam R um anel de cadeia à direita, I um ideal à direita de R, P um ideal à esquerda de R e $S = R \backslash P$. Então $I \subseteq IS^{-1} = \bigcup_{s \in S} Is^{-1}$, que é um ideal à direita de R. Se I é um ideal bilateral de R, então IS^{-1} também é ideal bilateral.*

Demonstração:

Seja $x \in IS^{-1}$. Então existe $s \in S$ tal que $xs \in I$. Consideremos $r \in R$ qualquer. Como R é anel de cadeia à direita temos que $rs \in sR$ ou $s \in rsR$. No primeiro caso existe $q \in R$ tal que $rs = sq$ e temos $xrs = xsq \in I$ pois $xs \in I$ e I é um ideal à direita. No segundo caso, existe $t \in R$ tal que $s = rst$.

Observemos que $t \notin P$ uma vez que P é ideal à esquerda e $s \notin P$. Segue que $xrst = xs \in I$ com $st \in S$. Portanto $xR \subseteq IS^{-1}$. Sejam $x, y \in IS^{-1}$. Então existem $s_1, s_2 \in S$ tais que $xs_1 \in I$ e $xs_2 \in I$. Como R é anel de cadeia, temos que $s_1 = s_2a$ ou $s_2 = s_1b$ para certos $a, b \in S$ pois se não estivessem em S teríamos que s_1 ou s_2 estariam em P, o que não pode ocorrer. Supondo que o primeiro caso valha temos: $(x + y)s_1 = xs_1 + ys_1 = xs_1 + ys_2a$. Segue que $(x + y)s \in I$, uma vez que $ys_2a \in I$ e $xs_1 \in I$. Portanto $(x + y) \in IS^{-1}$. O segundo caso é análogo. Com isso mostramos que IS^{-1} é um ideal à direita de R. Claramente temos que $I \subseteq IS^{-1}$ e que, se I é um ideal bilateral, então IS^{-1} é bilateral. □

Faremos agora algumas observações sobre o ideal à direita IS^{-1}. Primeiramente, se $I \cap S \neq 0$, então $1 \in IS^{-1}$ e $IS^{-1} = R$. Em vista disso, normalmente assumiremos que I está contido em um ideal à esquerda $P = R \backslash S$. Notemos também que para quaisquer ideais à direita I_1 e I_2 de R com $I_1 \subseteq I_2S^{-1}$ temos que $I_1S^{-1} \subseteq I_2S^{-1}$. A situação mais interessante é quando P é um ideal completamente primo do anel R, abordada abaixo.

Corolário 2.16. *Seja R um anel de cadeia à direita, $P = R \backslash S$ um ideal completamente primo e I um ideal bilateral contido em P. Então IS^{-1} é também um ideal bilateral e $(IS^{-1})S^{-1} = IS^{-1}$.*

Demonstração:

Como conseqüência direta do Lema 2.15 temos que IS^{-1} é um ideal bilateral de R. Resta mostrar que $(IS^{-1})S^{-1} = IS^{-1}$. Obviamente $(IS^{-1})S^{-1} \supseteq IS^{-1}$. Consideremos agora $x \in (IS^{-1})S^{-1}$. Então existem $s_1, s_2 \in S$ tais que $xs_1s_2 \in I$. Como S é fechado $s_1s_2 \in S$ e temos $x \in IS^{-1}$. Logo $(IS^{-1})S^{-1} = IS^{-1}$ e o corolário está provado. □

Notemos que na última etapa da demonstração acima, não utilizamos o fato de I ser um ideal bilateral de R. Isto quer dizer que $(IS^{-1})S^{-1} = IS^{-1}$ é válido quando I é apenas um ideal à direita de R.

Consideremos agora R um anel de cadeia à direita. Sejam I um ideal à direita de R e P um ideal completamente primo de R tais que $P \supseteq I$. O teorema que segue busca fazer uma relação entre IS^{-1} e IP onde $S = R \backslash P$. Para tanto vamos definir o seguinte ideal à direita, associado à I e P:

$$\Upsilon(I) = \bigcap_{x \in P} (IP)x^{-1} = \{r \in R \mid rP \subseteq IP\}.$$

É fácil ver que se I é um ideal bilateral, $\Upsilon(I)$ é o anulador à esquerda do R-módulo P/IP.

Lema 2.17. *Seja R um anel de cadeia à direita, $P = R \backslash S$ um ideal completamente primo de R e I um ideal à direita de R.*

(i) Para $I \subseteq aR \subseteq IS^{-1}$, temos $(aR)S^{-1} = IS^{-1}$.

(ii) $(IS^{-1})P = IP$.

(iii) Se $IP \subset I$, então $\Upsilon(I) = IS^{-1}$.

(iv) Se $IP \subset I$ vale, então, para todo $a \in I \backslash IP$, temos $aP = IP$.

(v) IP é um ideal bilateral se, e somente se, IS^{-1} é um ideal bilateral.

Demonstração:

(i) Consireremos $I \subseteq aR \subseteq IS^{-1}$. Segue que $IS^{-1} \subseteq (aR)S^{-1} \subseteq (IS^{-1})S^{-1} = IS^{-1}$, onde a última igualdade é valida pela observação feita após a prova do Corolário 2.16. Portanto $(aR)S^{-1} = IS^{-1}$.

(ii) Obviamente $I \subseteq IS^{-1}$. Daí $IP \subseteq (IS^{-1})P$. Para mostrar a outra contenção, suponhamos que $x \in IS^{-1}$. Então existe $s \in S$ tal que $xs \in I$. O Lema 2.14 nos garante que $IP \supseteq xsP = xP$. Como $x \in IS^{-1}$ é qualquer, temos que $(IS^{-1})P \subseteq IP$, e portanto $(IS^{-1})P = IP$.

(iii) Pelo ítem (ii) deste lema temos que $(IS^{-1})P = IP$. Portanto $\Upsilon(I) \supseteq IS^{-1}$. Consideremos agora $x \in \Upsilon(I)$. Então $xP \subseteq IP$. Tomando $a \in I \backslash IP$ temos $IP \subset aR \subseteq I$. Se ocorrer $x = ar$, para algum $r \in R$, então, para todo $s \in S$, teremos $xs = ars \in aR \subseteq I$, isto é, $x \in IS^{-1}$. Se ocorrer $a = xt$, para algum $t \in R$, então $t \notin P$, pois do contrário teríamos $a \in xP \subseteq IP \subseteq I$. Logo $x \in IS^{-1}$. Como $x \in \Upsilon(I)$ é qualquer, segue que $\Upsilon(I) \subseteq IS^{-1}$. Portanto, concluímos que $\Upsilon(I) = IS^{-1}$.

(iv) Seja $a \in I \backslash IP$. Então $aP \subseteq IP$. Suponhamos agora que $x \in I$. Vamos mostrar que $xP \subseteq aP$, para todo $x \in I$. Uma vez que R é anel de cadeia à direita, temos $xR \subseteq aR$ ou $aR \subseteq xR$. No primeiro caso $x = ar$, para algum $r \in R$. Daí $xP = arP \subseteq aP$. No segundo caso $a = xt$, para certo $t \in R$. Se $t \in P$, então $a = xt \in IP$, o que é um absurdo. Segue que $t \in S$. Pelo Lema 2.14, $P = tP$ e isto implica que $xP = xtP = aP$. Como $x \in I$ é qualquer, provamos que $aP \supseteq IP$ e portanto $aP = IP$.

(v) Suponhamos que IS^{-1} é um ideal bilateral de R. Então $(IS^{-1})P$ também é um ideal bilateral de R. Segue, pelo ítem (ii) deste lema que $(IS^{-1})P = IP$ e assim garantimos uma das implicações. Consideremos agora que IP é um ideal bilateral de R. Então $\Upsilon(I) = \{r \in R |\ rP \subseteq IP\}$ também é um ideal bilateral de R, pois dado $r \in \Upsilon(I)$, temos $rP \subseteq IP$. Logo $trP \subseteq IP$, para todo $t \in R$, uma vez que IP é bilateral. A partir deste momento, passamos a considerar dois casos. O primeiro é quando $IP \subset I$. Pelo ítem (iii) deste lema garantimos que $\Upsilon(I) = IS^{-1}$ e segue a bilateralidade deste último ideal. No segundo caso consideramos a igualdade $IP = I$ e caímos nas hipóteses do Corolário 2.16, concluindo assim a demonstração. $\square$

Corolário 2.18. *Seja R um anel de cadeia à direita, $0 \neq a \in R$, $P = R \backslash S$ um ideal completamente primo de R. Então as seguintes sentenças são equivalentes:*

(a) $(aR)S^{-1}$ *é um ideal bilateral de* R*.*

(b) aP *é um ideal bilateral de* R*.*

(c) $a \notin RaP$*.*

Demonstração:

$(a) \Leftrightarrow (b)$. Pelo ítem (v) do Lema 2.17 temos que $(aR)S^{-1}$ é um ideal bilateral de R se, e somente se, (aR)P é um ideal bilateral de R. Como P também é um ideal bilateral de R, temos $aRP = aP$ e segue o resultado.

$(b) \Rightarrow (c)$. Suponhamos, por absurdo, que $a \in RaP$. É válido que $RaP \subseteq aP$, pois aP é um ideal bilateral de R. Segue que $a \in aP$, isto é, existe $p \in P$ tal que $a = ap$ e daí $a(1-p) = 0$. Como $P \subseteq J(R)$, $1-p$ é invertível, e portanto $a = 0$, o que é um absurdo. Logo $a \notin RaP$.

$(c) \Rightarrow (a)$. Suponhamos que (c) verifica-se. Pelo Lema 2.15, $(aR)S^{-1}$ é um ideal à direita de R. Resta mostrar que também é um ideal à esquerda de R. Para tanto, consideremos $x \in (aR)S^{-1}$. Então existe $s \in S$ tal que $xs \in aR$. Segue que $xs = ab$, para algum $b \in R$. Seja $r \in R$. Para completar a demonstração, resta verificar que $rx \in (aR)S^{-1}$. Como R é anel de cadeia à direita, vale $rxsR \subseteq aR$ ou $aR \subseteq rxsR$. No primeiro caso não há o que provar pois $s \in S$. No segundo caso, existe $v \in R$ tal que $aR \ni a = r(xs)v = rabv$. Por hipótese $a \notin RaP$, portanto $bv \notin P$. Pelo fato de P ser completamente primo, temos que $v \in S$ e conseqüentemente $sv \in S$. Assim $(aR)S^{-1}$ é um ideal à esquerda de R. Logo é um ideal bilateral de R. $\square$

O corolário acima descreve uma relação entre $(aR)S^{-1}$ e aP.

Corolário 2.19. *Seja* R *um anel de cadeia à direita e* $P = R\backslash S$ *um ideal completamente primo de* R*. Então temos:*

(i) $(aR)S^{-1} = aR \cup \{x \in R \mid xs = a,$ *para algum* $s \in S\}$

(ii) *Seja* $0 \neq aR \subseteq bR$. *Então as seguintes sentenças são equivalentes:*

(a) $a = bs$, *para algum* $s \in S$.

(b) $(aR)S^{-1} = (bR)S^{-1}$.

(c) $aP = bP$.

Demonstração:

(i) Claramente a igualdade vale para $a = 0$. Suponhamos então $a \neq 0$. Obviamente $(aR)S^{-1} \supseteq aR \cup \{x \in R \mid xs = a \text{ } \textit{para algum} \text{ } s \in S\}$. Para mostrarmos a outra contenção, consideremos $x \in (aR)S^{-1} \backslash aR$ e $a \neq 0$. Como $x \notin aR$ e R é anel de cadeia, temos $a = xt$, para algum $t \in R$. Se $t \in S$ está provado. Se $t \notin S$, $t \in P$. Pelo fato de x pertencer a $(aR)S^{-1}$, existe $s \in S$ tal que $xs \in aR$ e isto implica que $xs = ar$, para algum $r \in R$. Substituindo a pela igualdade $a = xt$ segue que $xs = xtr$ e daí, $x(s - tr) = 0$. Usando que R é anel de cadeia, $s \notin P$ e $t \in P$ temos que $tr = sy$, onde $y \in R$, pois $sR \supset trR$. Observemos que obrigatoriamente $y \in P$, uma vez que $ts \in P$, $s \notin P$ e P é ideal completamente primo de R. Podemos agora substituir a igualdade acima na anterior e obtemos $x(s - sy) = 0$, isto é, $xs(1 - y) = 0$. Como $y \in P \subseteq J(R)$, $1 - y$ é invertível e conseqüentemente $xs = 0$. Lembrando novamente que R é anel de cadeia, podemos escrever $t = sz$, para algum $z \in R$, já que $s \notin P$. Com isso temos: $a = xt = xsz = (xs)z = (0)z = 0$, o que é um absurdo pois supomos que $a \neq 0$. Portanto, vale somente o primeiro caso onde a contenção é válida.

(ii) $(a) \Rightarrow (b)$ Afirmamos que $aR \subseteq bR \subseteq (aR)S^{-1}$. De fato, considerando que (a) é válido, isto é, $a = bs$, temos que $aR \subseteq bR$. Resta mostrar que $bR \subseteq (aR)S^{-1}$. Para tanto suponhamos que $x \in bR$. Daí $x = br$, para algum $r \in R$. Como R é anel de cadeia, $rR \subseteq sR$ ou $sR \subseteq rR$. Se $rR \subseteq sR$, então existe $t_1 \in R$ tal que $r = st_1$. Daí $x = br = bst_1 = (bs)t_1 = at_1 \in aR \subseteq$

$(aR)S^{-1}$. Se $sR \subseteq rR$, então $s = rt_2$, para algum $t_2 \in R$. Observemos que $t_2 \in S$, pois $s \in S = R \backslash P$. Segue que $aR \ni a = bs = b(rt_2) = (br)t_2 = xt_2$. Portanto $x \in (aR)S^{-1}$. Como $x \in bR$ é qualquer, a contenção é válida, e conseqüentemente $aR \subseteq bR \subseteq (aR)S^{-1}$. Usando o Lema 2.17($i$) concluímos $(aR)S^{-1} = (bR)S^{-1}$. Logo a implicação é verdadeira.

(b) $\Rightarrow$ (c) Suponhamos que $(aR)S^{-1} = (bR)S^{-1}$. Segue que $(aR)S^{-1}P = (bR)S^{-1}P$. Pelo Lema 2.17($ii$) temos $aRP = bRP$, ou seja, $aP = bP$, pois P é ideal bilateral de R.

(c) $\Rightarrow$ (a) Consideremos $aP = bP$. Como, por hipótese, $aR \subseteq bR$, temos que $a = bs$, para algum $s \in R$. Suponhamos, por absurdo, que $s \in P$. Então $aP \subseteq aR = bsR \subseteq bP = aP$. Isto implica que $aR = aP$, de onde segue que $a = 0$, o que é um absurdo. Portanto $a = bs$, para algum $s \in S$. $\square$

Os elementos a, $b \in R^*$ que satisfazem as condições do Corolário 2.19 (ii) são chamados *S-associados à direita* e abreviamos por $a \sim_S b$. Elementos *S-associados à esquerda* define-se similarmente.

Provaremos agora um teorema sobre ideais primos. Para tanto, necessitaremos do seguinte lema:

Lema 2.20. *Seja R um anel de cadeia à direita.*

(i) Se A é um ideal à direita de R, então não existe ideal primo P de R, tal que $\bigcap_{n \in \mathbb{N}} A^n \subset P \subset A$.

(ii) Se $t \in R$, então não existe ideal completamente primo P de R tal que $\bigcap_{n \in \mathbb{N}} t^n R \subset P \subset tR$.

Demonstração:

(i) Seja P um ideal primo de R, R satisfazendo as condições acima, e consideremos $n \in \mathbb{N}$ o mínimo tal que $A^n \subseteq P$. Como P é um ideal primo de

R temos que $n = 1$ e portanto $A \subset P$, o que é um absurdo. Logo não existe ideal primo P de R, tal que $\bigcap_{n\in\mathbb{N}} A^n \subset P \subset A$.

(ii) Sejam P um ideal completamente primo de R e $n \in \mathbb{N}$ o mínimo tal que $t^nR \subseteq P$. Então $t^n \in P$. Como P é completamente primo, temos que $t \in P$. Portanto $tR \subseteq P$. Logo não existe ideal completamente primo P de R tal que $\bigcap_{n\in\mathbb{N}} t^nR \subset P \subset tR$. □

Estes resultados fornecem exemplos de segmentos de ideais principais que não contém ideais primos. O teorema abaixo mostrará, com algumas hipóteses adicionais, que os limites desses segmentos são os melhores possíveis.

Teorema 2.21. *Seja R um anel de cadeia à direita.*

(i) Ideais bilaterais idempotentes de R diferentes de zero são completamente primos.

(ii) Se A é um ideal (bilateral) de R que não é nilpotente, então $P = \bigcap_{n\in\mathbb{N}} A^n$ é um ideal completamente primo de R.

(iii) Se $t \in J(R)$ não é nilpotente, então $P = \bigcap_{n\in\mathbb{N}} t^nR$ é um ideal primo à direita de R. E mais: se P é um ideal bilateral de R, então P é um ideal completamente primo de R.

Demonstração:

(i) Seja $0 \neq A = A^2$ um ideal idempotente de R. Para demonstrar este ítem usaremos o Lema 2.12(iii) que nos diz que se A é um ideal bilateral de R, A é um ideal completamente primo se, e somente se, $x^2 \in P$ implica $x \in P$. Para tanto, suponhamos por absurdo que $a \notin A$, mas $a^2 \in A$. Então $A \subseteq aJ(R)$, pois se existisse $a' \in A$ tal que $a' = au$, onde u é invertível, isto é, $u \in R\backslash A$ teríamos $a'u^{-1} = a$ que implicaria que $a \in A$, o que é um absurdo.

Segue que

$$A = A^2 = AA \subseteq aJ(R)A \subseteq aA \subseteq a(aJ(R)) = a^2J(R) \subset a^2R \subseteq A.$$

Com isso, as contenções se reduzem à igualdades e temos $a^2J(R) = a^2R$, o que também é um absurdo.

(ii) Seja $P = \bigcap_{n\in\mathbb{N}} A^n$. Temos dois casos a analisar: $P = A^n$, para algum $n \in \mathbb{N}$, e $P \subset A^n$, para todo $n \in \mathbb{N}$. No primeiro caso temos: $A \supseteq A^2 \supseteq ... \supseteq A^n \supseteq ... \supseteq A^{2n}$. Como $\bigcap_{n\in\mathbb{N}} A^n = P = A^n$ temos que $A^n \subseteq A^{2n}$. Segue que $A^n = A^{2n}$. Com isso estamos nas hipóteses do ítem (i) deste teorema, portanto $A^n = P$ é um ideal completamente primo de R. Suponhamos agora que $P \subset A^n$, para todo $n \in \mathbb{N}$. Mostraremos este caso usando a contrapositiva do Lema 2.12(iii). Para tanto, consideremos $t \in R$ tal que $t \notin P$. Como R é anel de cadeia à direita, existe $n \in \mathbb{N}$ tal que $A^n \subseteq tR$. Então $P \subset A^{2n} = A^nA^n \subseteq tRA^n \subseteq tA^n \subseteq ttR = t^2R$. Segue que $t^2 \notin P$, logo P é um ideal completamente primo de R.

(iii) Afirmamos que $t^{n+1}R \subset t^nR$. De fato, se valesse a igualdade teríamos $t^n = t^{n+1}r$ para algum $r \in R$ e isto implicaria que $t^n(1 - tr) = 0$. Como $t \in J(R)$, $1 - tr$ é invertível e seguiria que $t^n = 0$ o que, por hipótese, é impossível. Usaremos a contrapositiva do Lema 2.12(i) para mostrar esse ítem. Suponhamos que $x \notin P$. Como R é anel de cadeia à direita, existe $n \in \mathbb{N}$ tal que $t^nR \subseteq xR$. Com isso temos: $P \subset t^{2n}R = t^nt^nR \subseteq t^nxR \subseteq xRxR$. Se $xRx \in P$, teríamos $P \subset t^{2n} \subseteq xRxR \subseteq P$, e conseqüentemente $P = t^{2n}R$, o que é um absurdo. Portanto $P = \bigcap_{n\in\mathbb{N}} t^nR$ é um ideal primo à direita de R. Resta mostrar que se P é um ideal bilateral de R, então P é um ideal completamente primo de R. Provaremos usando a contrapositiva do Lema 2.12(iii). Para tanto, consideremos P ideal bilateral de R e $x \notin P$. Pelo fato de R ser um anel de cadeia à direita, existem $n \in \mathbb{N}$ e $a \in R$ tais que $t^n = xa$.

Segue que $t^{2n} = t^n t^n = xaxa = x(ax)a$. Novamente pelo fato de R ser anel de cadeia à direita temos $axR \subseteq xR$ ou $xR \subseteq axR$. No primeiro caso existe $b \in R$ tal que $ax = xb$. Daí $t^{2n} = x(ax)a = x(xb)a = x^2ba$. Suponhamos agora, por absurdo, que $x^2 \in P$, então $P \subset t^{2n}R = x^2baR \subseteq P$. Assim $P = t^{2n}R$, o que é impossível graças a afirmação inicial. Portanto, neste caso teríamos $x^2 \notin P$. Na outra possibilidade consideremos apenas $xR \subset axR$. Segue que $x = axr$, para algum $r \in J(R)$. O fato de x não pertencer a P implica que $xr \notin P$, pois P é um ideal bilateral. Então existem $m \in \mathbb{N}$ e $q \in R$ tais que $t^m = xrq$. Com isso obtemos: $x^2q = x(x)q = x(axr)q = (xa)(xrq) = t^n t^m = t^{n+m}$. Supondo, por absurdo, que $x^2 \in P$ temos $P \subset t^{n+m}R = x^2qR \subseteq P$, o que é uma contradição. Portanto $x^2 \notin P$ e concluímos que P é um ideal completamente primo de R. $\square$

Lema 2.22. *Sejam R um anel de cadeia (à direita e à esquerda) P um ideal não nulo e completamente primo de R, que é principal à direita. Então P é igual ao ideal maximal $J(R)$.*

Demonstração:

Suponhamos, por absurdo, que $P = pR \subset J(R)$. Consideremos um elemento qualquer $a \in J(R) \backslash P$. Como R é anel de cadeia, temos $P = Pa$, pela versão simétrica do Lema 2.14. Segue que $pR = P = Pa = (pR)a = p(Ra) \subseteq pJ(R)$, onde a última contenção é garantida pelo fato de J(R) ser um ideal bilateral de R. Obtemos então $pR = pJ(R)$ uma vez que $pJ(R) \subseteq pR$ vale obviamente. Portanto existe $j \in J(R)$ tal que $p = pj$ e isto implica que $p = 0$, uma contradição. Logo P é igual ao ideal maximal $J(R)$. $\square$

Capítulo 3

Anéis e Módulos Distributivos

Este capítulo é baseado no trabalho de Stephenson [16], abrangendo, basicamente, as seções 1 e 2. Sua finalidade é dar uma caracterização de módulos distributivos à direita, aplicando esses resultados à anéis distributivos à direita.

Usaremos neste capítulo a notação R_R para indicar R como um R-módulo à direita. Distributividade aqui sempre significará distributividade à direita, a menos que se diga algo em contrário.

3.1 Módulos Distributivos.

Nesta seção estaremos interessados em caracterizar módulos distributivos à direita.

Definição 3.1. *Sejam M um R-módulo à direita e $\mathcal{L}(M)$ o reticulado dos submódulos de M. Então M é um módulo distributivo se $\mathcal{L}(M)$ é um reticulado distributivo, isto é,* *(i) para todo* A, B, $C \in \mathcal{L}(M)$, $A \cap (B + C) = (A \cap B) + (A \cap C)$ *ou equivalentemente*

(ii) para todo A, B, $C \in \mathcal{L}(M)$, $A + (B \cap C) = (A + B) \cap (A + C)$.

Para a próxima demonstração usaremos o fato de que o reticulado de um módulo é distributivo se, e somente se, seus complementos relativos são únicos, isto é, o reticulado dos submódulos não possui subreticulados da forma:

$$
\begin{tikzcd}[column sep=small]
 & E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & B \arrow[d, dash] & C \arrow[dl, dash] \\
 & D &
\end{tikzcd}
$$

onde A, B, C, D e E são submódulos de um módulo M.

Daremos aqui apenas uma idéia desta demonstração. O leitor interessado pode encontrar a demonstração completa em ([4], Chapter 2, Corollary 4.6 ou em [9]).

Consideremos, então, que o reticulado de um certo R-módulo M é distributivo e suponhamos, por absurdo, que ele contém um subreticulado da forma descrita pela figura acima. É fácil ver que $(A \cap B) + (B \cap C) + (C \cap A) = (A + B) \cap (B + C) \cap (C + A)$. Mas $(A \cap B) + (B \cap C) + (C \cap A) = D + D + D = D$ e $(A + B) \cap (B + C) \cap (C + A) = E \cap E \cap E = E$. Com isso temos $D = E$, o que é um absurdo.

Reciprocamente, suponhamos que o reticulado não é distributivo. A partir dessa hipótese é possível construir um reticulado igual à figura acima e então fica demonstrada a afirmação. De fato pois, como o reticulado não é distributivo, facilmente vemos que $(X\cap Y)+(Y\cap Z)+(Z\cap X) \neq (X+Y)\cap(Y+Z)\cap(Z+X)$ e que $(X\cap Y)+(Y\cap Z)+(Z\cap X) \subseteq (X+Y)\cap(Y+Z)\cap(Z+X)$, onde X, Y e Z são submódulos de M. Considerando $D = (X \cap Y) + (Y \cap Z) + (Z \cap X)$, $E = (X+Y)\cap(Y+Z)\cap(Z+X)$ e tomando $A = (E\cap X)+D$, $B = (E\cap Y)+D$ e $C = (E \cap Z) + D$ podemos construir, mediante alguns cálculos, um reticulado que possui a forma da figura acima. Logo um módulo é distributivo se, e somente se, seus complementos relativos são únicos.

Proposição 3.2. *Seja M um R-módulo à direita. Então M é um módulo distributivo se, e somente se, $Hom(A/(A \cap B), B/(A \cap B) = 0$, para todo A, $B \in \mathcal{L}(M)$.*

Demonstração:

Suponhamos inicialmente que $A \cap B = 0$. Começamos a demonstração afirmando que existe uma bijeção entre $Hom(A, B)$ e o conjunto dos complementos de B em $A \oplus B$, para todo $A, B \in \mathcal{L}(M)$([15], Lemma 1). De fato, consideremos $\varphi : Hom(A, B) \longrightarrow \{X \in \mathcal{L}(M) \mid X \oplus B = A \oplus B\}$ dada por $\varphi(\alpha) = Ker(\alpha^*)$, onde $\alpha^* : A \oplus B \longrightarrow B$ é tal que $\alpha^*|_A = \alpha$ e $\alpha^*|_B = id$ (isto é, α^* é uma projeção de $A \oplus B$ em B). Para verificar a injetividade, consideremos $\alpha, \beta \in Hom(A, B)$ tais que $Ker(\alpha^*) = Ker(\beta^*)$. Tomando $a \in A$, temos $\alpha(a) \in B$, $\alpha^*(\alpha(a)) = \alpha(a)$ e $\alpha^*(a) = \alpha(a)$. Segue que $\alpha^*(a - \alpha(a)) = 0$. Portanto $a - \alpha(a) \in Ker(\alpha^*) = Ker(\beta^*)$. Conseqüentemente $0 = \beta^*(a-\alpha(a)) = \beta^*(a)-\beta(\alpha(a)) = \beta(a)-\alpha(a)$ e isto implica que $\alpha(a) = \beta(a)$. Como $a \in A$ é qualquer, $\alpha = \beta$, isto é, φ é injetiva. Seja, agora, $X \in \mathcal{L}(M)$ tal que $X \oplus B = A \oplus B$. Consideremos p a projeção de $X \oplus B$ em B em relação a X. Então $Ker(p) = X$. Chamando $\alpha = p|_A : A \longrightarrow B$. Segue que $\alpha^* = p$, pois $\alpha^*|_A = p|_A = \alpha$ e $\alpha^*|_B = p|_B = id$. Portanto φ é sobrejetiva. Logo φ é bijetiva. Usando este resultado e a afirmação feita antes dessa proposição, temos que $Hom(A, B) = 0$, quando $A \cap B = 0$. Com isso, o resultado segue claramente. $\square$

Desta proposição seguem os seguintes corolários:

Corolário 3.3. *Sejam A e B submódulos de um R-módulo à direita distributivo M.*

(i) Se $A + B = M$ então $Hom(M/B, M/A) = 0$.

(ii) Se $A \cap B = 0$ então $Hom(A, B) = 0$.

Demonstração:

(i) Do teorema dos homomorfismos temos que $N/(N \cap P) \simeq (N + P)/P$, onde N e P são submódulos de M. Assim temos $A/(A \cap B) \simeq (A + B)/B = M/B$ e $B/(A \cap B) \simeq (A + B)/A = M/A$, para todo A, $B \in L(M)$. Logo, pela Proposição 3.2, $0 = Hom(A/(A \cap B), B/(A \cap B) = Hom(M/B, M/A)$, para todo A, $B \in L(M)$.

(ii) O resultado segue direto da Proposição 3.2. $\square$

Para demonstrar o próximo corolário, necessitamos da seguinte definição:

Lembremos que um elemento $a \in R$ é dito um elemento central se a comuta com todo elemento de R.

Corolário 3.4. *Todo elemento idempotente de um anel distributivo à direita é central.*

Demonstração:

Seja e um elemento idempotente de R, onde R é um anel distributivo à direita. Afirmamos inicialmente que $Hom_R(eR, (1 - e)R) \simeq (1 - e)Re$, como grupos aditivos. De fato, basta definirmos $\lambda : Hom_R(eR, (1 - e)R) \longrightarrow (1 - e)Re$ por $\lambda(f) = f(e)$, para todo $f \in Hom_R(eR, (1 - e)R)$. O homomorfismo

λ está bem definido pois $f(e) = f(e^2) = f(e)e \in (1-e)Re$. Além disso, se $f(e) = g(e)$, então, para todo $r \in R$, $f(er) = f(e)r = g(e)r = g(er)$, ou seja, $f = g$. Portanto λ é injetora. Mostremos agora a sobretividade. Para tanto, tomemos $(1-e)xe \in (1-e)Re$. Consideremos $h : eR \longrightarrow (1-e)R$ definida por $h(er) = (1-e)xer$. Segue que $(1-e)xe = h(e) = \lambda(h)$ e obtemos que λ é sobrejetiva. Agora, pelo Lema 1.5 obtemos que $R = eR \oplus (1-e)R$. Com isso segue, do Corolário 3.3(ii), que $Hom(eR, (1-e)R) = 0$ e portanto $(1-e)Re = 0$, ou seja, $(1-e)re = 0$, para todo $r \in R$ o que implica que $er = ere$, para todo $r \in R$. Analogamente mostra-se que $eR(1-e) = 0$, ou seja $er = ere$, para todo $r \in R$. Logo $er = ere = re$, para todo $r \in R$. $\square$

Dado um R-módulo M, onde R é um anel, consideremos dois conjuntos que terão muita utilidade para o que se segue e são uma extensão do caso particular da Definição 1.16. São eles o *anulador à esquerda de* $x \in M$ que é o conjunto $l(x) = \{r \in R : rx = 0\}$ e o *anulador à direita de* $x \in M$, dado por $r(x) = \{r \in R : xr = 0\}$. Claramente, estes conjuntos são ideais à esquerda e à direita respectivamente.

Definimos abaixo o conceito de Domínio de Ore e de submódulos essenciais, necessários para o próximo corolário.

Definição 3.5. *Um domínio R que satisfaz $aR \cap bR \neq 0$ ($Ra \cap Rb \neq 0$), para todos elementos $a, b \in R$, é chamado Domínio de Ore à direita (à esquerda).*

Equivalentemente, na definição acima poderíamos dizer que $A \cap B \neq 0$ para todos ideais à direita (à esquerda) diferentes de zero.

Definição 3.6. *Sejam R um anel, M um R-módulo à direita e P um submódulo. P é chamado de submódulo essencial de M se $P \cap Q \neq 0$, para todo $Q \in \mathcal{L}(M)$, com $Q \neq 0$. Se todo submódulo $P \in \mathcal{L}(M)$ é um submódulo essencial, então M é chamado de módulo uniforme.*

Notemos que dizer que um domínio R visto como R-módulo à direita (à esquerda), é um módulo uniforme, é o mesmo que dizer que R é um domínio de Ore à direita (esquerda).

Corolário 3.7. *Suponhamos que M é um R-módulo à direita distributivo e $m \in M$. Se $r(m) = 0$ então mR é um submódulo essencial de M. Em particular, qualquer domínio distributivo à direita é um domínio de Ore à direita.*

Demonstração:

Sejam R um anel, M um R-módulo distributivo e $m \in M$. Começamos a demonstração afirmando que se $r(m) = 0$, então $R \simeq mR$. De fato, pois claramente o homomorfismo $\varphi : R \longrightarrow mR$, dado por $\varphi(x) = mx$ é sobrejetivo. Então $R/Ker(\varphi) \simeq mR$. Mas $Ker(\varphi) = 0$, uma vez que $r(m) = 0$. Logo $R \simeq mR$. Suponhamos agora que existe $P \in \mathcal{L}(M)$, tal que $mR \cap P = 0$. Segue do Corolário 3.3(ii) que $Hom(mR, P) = 0$, isto é, $Hom(R, P) = 0$. Conseqüêntemente $P = 0$ pois, para todo $x \in P$, podemos definir o homomorfismo $\psi_x : R \longrightarrow P$ por $\psi_x(1) = x$. Como o homomorfismo é zero, obtemos $x = 0$. Logo mR é um submódulo essencial de M. Para terminar a demonstração, tomemos R um domínio distributivo à direita. Considerando R como um R-módulo à direita e observando que $r(x) = 0$, para todo $x \in R$, segue diretamente pelo que foi mostrado acima e pela observação após a última definição que R é um domínio de Ore à direita. $\square$

Antes do próximo corolário, definimos:

Definição 3.8. *Sejam R um anel, M um R-módulo à direita e P um submódulo. P é um submódulo totalmente invariante de M se $\alpha(P) \subseteq P$, para todo $\alpha \in End(M)$.*

Corolário 3.9. *Seja M um módulo à direita distributivo. Então qualquer submódulo maximal ou minimal à direita de M é totalmente invariante. Em particular, qualquer ideal maximal ou minimal à direita de um anel distributivo à direita é bilateral.*

Demonstração:

Suponhamos que P é um submódulo maximal de M e, por absurdo, que $\alpha(P) \nsubseteq P$, para algum $\alpha \in End(M)$. Como $\alpha(P) \nsubseteq P$ segue que $\alpha(M) + P$ possui elementos que não estão em P. Pelo fato de P ser maximal e de $\alpha(M)+P$ ser um submódulo temos que $\alpha(M)+P = M$. Afirmamos que $M/\alpha^{-1}(P) \simeq (\alpha(M)+P)/P = M/P$. De fato, definimos $\psi : M \longrightarrow (\alpha(M)+P)/P$ dada por $\psi(m) = \alpha(m) + P$, para todo $m \in M$. Claramente ψ é um homomorfismo e pelo fato de α estar bem definida, ψ também está bem definida. Para verificar a sobrejetividade, consideremos $a \in (\alpha(M)+P)/P$. Então $a = \alpha(m)+p+P = \alpha(m)+P$, para certos $\alpha(m) \in \alpha(M)$ e $p \in P$. Portanto , basta tomarmos $m \in M$ e temos $\psi(m) = \alpha(m)+P = \alpha(m)+p+P = a$, isto é, ψ é sobrejetiva. Pelo teorema dos isomorfismos vale $M/Ker(\psi) \simeq (\alpha(M) + P)/P = M/P$. Resta mostrar que $Ker(\psi) = \alpha^{-1}(P)$. Obviamente $Ker(\psi) \supseteq \alpha^{-1}(P)$. Seja $m \in Ker(\psi)$. Então $\psi(m) = \alpha(m) \in P$ e isto implica que $m \in \alpha^{-1}(P)$. Portanto $Ker(\psi) = \alpha^{-1}(P)$ e conseqüentemente $M/\alpha^{-1}(P) \simeq M/P$. Observemos que $\alpha^{-1}(P)$ é maximal, uma vez que P é maximal. Notemos também que $\alpha(P) \nsubseteq P$ implica que $P \nsubseteq \alpha^{-1}(P)$ pois se $P \subseteq \alpha^{-1}(P)$, teríamos $\alpha(P) \subseteq \alpha(\alpha^{-1}(P)) \subseteq P$, o que é uma contradição. Unindo os fatos de que $\alpha^{-1}(P)$ é maximal e $P \nsubseteq \alpha^{-1}(P)$ obtemos $P+\alpha^{-1}(P) = M$ e isto contraria o Corolário 3.3(i). Logo qualquer submódulo maximal de M é completamente invariante. Para finalizar a prova, basta considerar R como um R-módulo à direita e o homomorfismo $\alpha_a : R \longrightarrow R$ definido por $\alpha_a(x) = ax$, para todo $x \in R$, onde $a \in R$ está fixo. Consideremos I um ideal maximal à direita de R. Então

$\alpha_a(I) = aI \subseteq I$. Como $a \in R$ é qualquer segue que I é um ideal bilateral. Para o caso minimal a demonstração é análoga. $\square$

Uma conseqüência imediata desse corolário é que todo ideal maximal de um anel distributivo é completamente primo. Para verificarmos este fato, consideremos R um anel distributivo e P um ideal maximal de R. Consideremos ainda $a, b \in R$ com $a.b \in P$ e $b \notin P$. Como $b \notin P$, temos que $P + bR = R$, isto, é, existem $r \in R$ e $x \in P$ tais que $x + br = 1$. Segue que $a = a.1 = a.(x + br) = ax + abr \in P$. Logo P é um ideal completamente primo de R.

Agora daremos condições necessárias e suficientes para somas diretas de módulos distributivos serem também módulos distributivos. Para tanto, necessitamos de alguns resultados.

Definição 3.10. *Sejam R um anel, M um R-módulo à direita. Dois submódulos A e B são ditos não relacionados sempre que valer: dados $P' \subseteq P \subseteq A$ e $Q' \subseteq Q \subseteq B$ tais que $P/P' \simeq Q/Q'$, então $P = P'$ e $Q = Q'$, com Q, Q', P, P' submódulos de M.*

Lema 3.11. *Sejam R um anel, M um R-módulo à direita, e A e B submódulos de M. Então, A e B são não relacionados se, e somente se, $Hom(X/X', Y/Y') = 0$, para todos submódulos $X' \subseteq X \subseteq A$ e $Y' \subseteq Y \subseteq B$.*

Demonstração:

Suponhamos que $Hom(X/X', Y/Y') = 0$ e que $X/X' \simeq Y/Y'$. Segue diretamente do isomorfismo que $X = X'$ e $Y = Y'$. Seja $\alpha \in Hom(X/X', Y/Y')$. Daí, $Ker(\alpha)$ e $Im(\alpha)$ são da forma N/X' e Z/Y' respectivamente onde N e Z são tais que $X' \subseteq N \subseteq X \subseteq A$ e $Y' \subseteq Z \subseteq Y \subseteq B$. Segue do teorema dos isomorfismos que $X/N \simeq (X/X')/(N/X') \simeq Im(\alpha) = Z/Y'$. Do fato que A e B são não relacionados, segue que $N = X$ e $Z = Y'$. Logo $\alpha \equiv 0$. $\square$

O próximo lema nos dá uma outra caracterização de módulos não relacionados que generalizaremos na próxima proposição. Antes de demonstrá-lo, apresentaremos uma definição que facilitará nossa escrita.

Definição 3.12. *Sejam M um R-módulo à direita, X um submódulo de M e $y \in M$. Definimos o condutor à direita de y em X, como sendo o conjunto dado por $(X : y) = \{r \in R : yr \in X\}$.*

Lema 3.13. ([6], Lema 2.1) *Seja R um anel e $A_1 \oplus A_2$ uma soma direta de dois R-módulos à direita. Então as seguintes sentenças são equivalentes:*

(i) Todo submódulo de $A_1 \oplus A_2$ é da forma $C \oplus D$, para algum $C \in \mathcal{L}(A_1)$ e para algum $D \in \mathcal{L}(A_2)$.

(ii) $r(x) + r(y) = R$, para todo $x \in A_1$ e $y \in A_2$.

(iii) $Hom_R(X/X', Y/Y') = 0$, para todos submódulos à direita $X' \subseteq X \subseteq A_1$ e $Y' \subseteq Y \subseteq A_2$, isto é, A_1 e A_2 são não relacionados.

Demonstração:

$(i) \Rightarrow (ii)$ Seja W um submódulo qualquer de $A_1 \oplus A_2$. Então $W = C \oplus D$ para algum submódulo à direita C de A_1 e para algum submódulo à direita D de A_2. Observemos que $W \cap A_1 = (C \oplus D) \cap A_1 = C \oplus 0$ e $W \cap A_2 = (C \oplus D) \cap A_2 = 0 \oplus D$. Segue disto que $W = C \oplus D = (C \oplus 0) + (0 \oplus D) = (W \cap A_1) + (W \cap A_2)$. Consideremos agora o submódulo $(x+y)R$ de $A_1 \oplus A_2$, onde $x \in A_1$ e $y \in A_2$ são quaisquer. Pelo mesmo argumento acima temos: $(x+y)R = ((x+y)R \cap A_1) + ((x+y)R \cap A_2)$. Segue que $x + y = u + v$ para algum $u \in (x+y)R \cap A_1$ e $v \in (x+y)R \cap A_2$. Afirmamos que $x = u$ e $y = v$. De fato, pois notemos que $(x + y) - (x + v) = (u + v) - (x + v)$. Com isso obtemos $0 + (y - v) = (u - x) + 0$, isto é, $(y - v) = 0$ e $(u - x) = 0$. Segue que $y = v$ e $u = x$. Mas $u \in (x+y)R \cap A_1$ e $v \in (x+y)R \cap A_2$ e isto implica que $x = u = (x+y)s_1 \in A_1$ e $y = v = (x+y)s_2 \in A_2$, para certos $s_1, s_2 \in R$.

Daí $x(1-s_1) = ys_1 \in A_1 \cap A_2 = 0$ e segue que $1 - s_1 \in r(x)$ e $s_1 \in r(y)$. Conseqüentemente $1 = (1-s_1) + s_1 \in r(x) + r(y)$. Logo $r(x) + r(y) = R$.

$(ii) \Rightarrow (i)$ Seja U um submódulo à direita de $A_1 \oplus A_2$. Então, para todo $u \in U$, temos $u = m+n$ para certos $m \in A_1$ e $n \in A_2$. Como $r(m)+r(n) = R$, $1 = a + b$ para algum $a \in r(m)$ e para algum $b \in r(n)$. Segue que $ub = (m+n)b = mb+nb = mb \in U \cap A_1$ e $ua = (m+n)a = ma+na = na \in U \cap A_2$. Temos ainda que $m = m.1 = m(a+b) = ma+mb = mb$ e $n = n.1 = n(a+b) = na+nb = na$. Portanto $u = m+n = mb+na = ub+ua \in (U \cap A_1) \oplus (U \cap A_2)$. Como $u \in U$ é arbritário, obtemos $U = (U \cap A_1) \oplus (U \cap A_2)$.

$(ii) \Rightarrow (iii)$ Por absurdo, suponhamos que existem submódulos à direita $X_2 \subseteq X_1$ de A_1 e $Y_2 \subseteq Y_1$ de A_2 tais que $Hom_R(X_1/X_2, Y_1/Y_2) \neq 0$, isto é, existe um homomorfismo $f : X_1/X_2 \longrightarrow Y_1/Y_2$ não nulo. Conseqüentemente, existe um elemento $x_1 \in X_1 \backslash X_2$ tal que $f(x_1+X_2) = y_1+Y_2$ com $y_1 \in Y_1/Y_2$. Notemos agora que $r(x_1) \subseteq (X_2 : x_1) = r(x_1+X_2)$ e $r(y_1) \subseteq (Y_2 : y_1) = r(y_1+ Y_2)$. Mas $r(x_1)+r(y_1) = R$. Portanto $r(x_1+X_2)+r(y_1+Y_2) = R$. Obsevemos que, tomando $t \in r(x_1 + X_2)$, temos $f(x_1 + X_2).t = f((x_1 + X_2)t) = 0$ em Y_1/Y_2 uma vez que f é um homomorfismo e isto implica que $r(x_1 + X_2) \subseteq r(f(x_1 + X_2)) = r(y_1 + Y_2)$. Segue disto que $r(y_1 + Y_2) = r(f(x_1 + X_2)) = R$ e conseqüentemente $f(x_1 + X_2) = 0$ em Y_1/Y_2, o que é uma contradição. Logo, devemos ter $Hom_R(X/X', Y/Y') = 0$, para todos submódulos à direita $X' \subseteq X \subseteq A_1$ e $Y' \subseteq Y \subseteq A_2$, isto é, A_1 e A_2 são não relacionados.

$(iii) \Rightarrow (ii)$ Por absurdo, suponhamos que existam $m \in A_1$ e $n \in A_2$ tais que $r(m) + r(n) \neq R$. Definimos agora os seguintes homomorfismos entre R-módulos à direita que, pelo fato de que $r(m) \subseteq r(m) + r(n)$ e $r(n) \subseteq r(m) + r(n)$, estão bem definidos: $f_1 : mR \simeq R/r(m) \longrightarrow R/(r(m) + r(n))$ e $f_2 : nR \simeq R/r(n) \longrightarrow R/(r(m) + r(n))$. Como $mR/Ker(f_1) \simeq R/(r(m) +$

$r(n))$ e $nR/Ker(f_2) \simeq R/(r(m)+r(n))$ e $r(m)+r(n) \neq R$, segue que existe um homomorfismo não nulo de $mR/Ker(f_1)$ em $nR/Ker(f_2)$, o que é uma contradição. Logo $r(m)+r(n) = R$, para todo $m \in A_1$ e $n \in A_2$. $\square$

Proposição 3.14. *Para uma família de módulos $(A_i)_{i\in I}$ as seguintes sentenças são equivalentes:*

(i) A_i é não relacionado com A_j, para todo $i \neq j \in I$.

(ii) Para todo submódulo X de $\oplus_I A_i$ temos $X = \oplus_I (X \cap A_i)$.

Demonstração:

$(i) \Rightarrow (ii)$ Consideremos $\oplus_I A_i$, onde A_i e A_j são não relacionados se $i \neq j$. Podemos supor, sem perda de generalidade, I finito, pois $X = \sum_F X \cap (\oplus_F A_i)$, onde F percorre todos os subconjuntos finitos de I. Assim, vamos supor $I = \{1, 2, 3, ..., n\}$ e vamos raciocinar por indução em n. Pelo lema anterior, o caso para $n = 2$ está demonstrado. Suponhamos agora que para um certo índice n fixo todo submódulo X de $\oplus_{i=1}^n A_i$ é da forma $X = \oplus_{i=1}^n (X \cap A_i)$ e mostremos que, para um submódulo W de $\oplus_{i=1}^{n+1} A_i$ é da forma $W = \oplus_{i=1}^{n+1} (W \cap A_i)$. Novamente pelo lema anterior temos: $W = W \cap \oplus_{i=1}^{n+1} A_i = W \cap ((\oplus_{i=1}^n A_i) \oplus A_n) = (W \cap \oplus_{i=1}^n A_i) \oplus (W \cap A_n)$. Claramente $W \cap \oplus_{i=1}^n A_i$ é submódulo de $\oplus_{i=1}^n A_i$. Então, pela hipótese de indução $W \cap \oplus_{i=1}^n A_i = \oplus_{i=1}^n [(W \cap \oplus_{i=1}^n A_i) \cap A_i] = \oplus_{i=1}^n W \cap A_i$. Logo $W = \oplus_{i=1}^{n+1} W \cap A_i$.

$(ii) \Rightarrow (i)$ Suponhamos que todo submódulo X de $\oplus_I A_i$ pode ser escrito como $X = \oplus_I (X \cap A_i)$. Em particular, todo submódulo X' de $A_k \oplus A_j$, com $A_k, A_j \in (A_i)_{i\in I}$, $k \neq j$, pode ser escrito como $X' = (X' \cap A_k) \oplus (X' \cap A_j)$. Então, pelo lema anterior, $Hom(B/B', C/C') = 0$, para todos submódulos $B' \subseteq B \subseteq A_k$ e $C' \subseteq C \subseteq A_j$. Logo, pelo Lema 3.13, A_k e A_j são não relacionados, para todo $k \neq j$. $\square$

Agora consideremos o caso em que os módulos são distributivos.

Proposição 3.15. *Para uma família de módulos distributivos $(A_i)_{i\in I}$ as seguintes sentenças são equivalentes:*

(i) $\oplus_I A_i$ *é um módulo distributivo.*

(ii) A_i *é não relacionado com* A_j*, para todo* $i \neq j \in I$

Demonstração:

$(i) \Rightarrow (ii)$ Suponhamos que $\oplus_I A_i$ é um módulo distributivo e $X \subseteq \oplus_I A_i$ é um submódulo. Então $X = \sum_F (X \cap A_i)$ quando F percorre subconjuntos finitos de I. Daí (ii) segue diretamente da proposição anterior.

$(ii) \Rightarrow (i)$ Suponhamos que C, D e E são submódulos de $\oplus_I A_i$. Então, pela proposição anterior, $C\cap(D+E) = (\oplus_I(C\cap A_i))\cap(\oplus_I(D\cap A_i)+\oplus_I(E\cap A_i)) = \oplus_I((C\cap A_i)\cap((D\cap A_i)+(E\cap A_i)))$. Pelo fato de A_i ser um módulo distributivo para todo $i \in I$ segue que $C \cap (D+E) = \oplus_I((C\cap A_i)\cap(D\cap A_i)+(C\cap A_i)\cap(E\cap A_i)) = \oplus_I((C\cap D)\cap A_i + (C\cap E)\cap A_i) = (C\cap D)+(C\cap E)$. Logo $\oplus_I A_i$ é um módulo distributivo. $\square$

O próximo lema nos dá uma caracterização de módulos distributivos através de homomorfismos.

Lema 3.16. *Para um módulo à direita* M *as seguintes sentenças são equivalentes:*

(i) M *é um módulo distributivo.*

(ii) Para todo módulo P *e* $\alpha \in Hom(P, M)$, $\alpha^{-1}(A+B) = \alpha^{-1}(A) + \alpha^{-1}(B)$, *para todo* $A, B \in \mathcal{L}(M)$.

(iii) Para todo módulo Q *e* $\alpha \in Hom(M, Q)$, $\alpha(A\cap B) = \alpha(A)\cap\alpha(B)$, *para todo* $A, B \in \mathcal{L}(M)$.

Demonstração:

$(ii) \Rightarrow (i)$ Inicialmente observemos que se P e C são submódulos e $\alpha : C \longrightarrow M$ é o homomorfismo inclusão, então claramente temos $\alpha^{-1}(P) = P \cap C$. Consideremos agora A, B, C submódulos de M. Daí $(A+B) \cap C = \alpha^{-1}(A+B) = \alpha^{-1}(A) + \alpha^{-1}(B) = (A \cap C) + (B \cap C)$, onde $\alpha : C \longrightarrow M$ é o homomorfismo inclusão . Logo M é um módulo distributivo.

$(i) \Rightarrow (ii)$ Consideremos M um módulo à direita distributivo, $A, B \in \mathcal{L}(M)$ e $\alpha \in Hom(P, M)$. Observemos que $\alpha^{-1}(A)+\alpha^{-1}(B) = \alpha^{-1}(\alpha(\alpha^{-1}(A)))+\alpha^{-1}(\alpha(\alpha^{-1}(B))) = \alpha^{-1}(\alpha(\alpha^{-1}(A))+\alpha(\alpha^{-1}(B)))$. Afirmamos que $\alpha(\alpha^{-1}(A)) = A \cap \alpha(P)$, para todo $A \in \mathcal{L}(M)$. De fato, seja $m \in \alpha(\alpha^{-1}(A))$. Então existe $n \in \alpha^{-1}(A) \subseteq P$ tal que $\alpha(n) = m$. Assim $n \in P$ é tal que $\alpha(n) \in A$. Segue daí que $m = \alpha(n) \in A \cap \alpha(P)$. Para a outra contenção, consideremos $x \in A \cap \alpha(P)$. Como $x \in A$ temos $\alpha^{-1}(x) \subseteq \alpha^{-1}(A)$ e segue que $x \in \alpha(\alpha^{-1}(x)) \subseteq \alpha(\alpha^{-1}(A))$, e está provada a afirmação. Assim: $\alpha^{-1}(A) + \alpha^{-1}(B) = \alpha^{-1}(\alpha(\alpha^{-1}(A)) + \alpha(\alpha^{-1}(B))) = \alpha^{-1}(A \cap \alpha(P) + B \cap \alpha(P)) = \alpha^{-1}((A+B) \cap \alpha(P)) = \alpha^{-1}(\alpha(\alpha^{-1}(A+B))) = \alpha^{-1}(A+B)$, pois M é distributivo. Logo para todo módulo P e $\alpha \in Hom(P, M)$, $\alpha^{-1}(A+B) = \alpha^{-1}(A) + \alpha^{-1}(B)$, para todo $A, B \in \mathcal{L}(M)$.

$(i) \Rightarrow (iii)$ Sejam M um módulo distributivo, Q um módulo qualquer e $\alpha \in Hom(M, Q)$. Consideremos $A, B \in \mathcal{L}(M)$. Então $\alpha(A \cap B) = [\alpha(A \cap B)] \cap Im(\alpha) = \alpha(\alpha^{-1}(\alpha(A \cap B)))$, onde a última igualdade é válida pois $\alpha(\alpha^{-1}(X)) = X \cap Im(\alpha)$, para todo homomorfismo α e para todo X submódulo de M. Afirmamos agora que o fato de M ser distributivo implica que $\alpha^{-1}(\alpha(A \cap B)) = \alpha^{-1}(\alpha(A) \cap \alpha(B))$. De fato, pois $\alpha^{-1}(\alpha(A \cap B)) = (A \cap B) + Ker(\alpha) = (A + Ker(\alpha)) \cap (B + Ker(\alpha)) = \alpha^{-1}(\alpha(A)) \cap \alpha^{-1}(\alpha(B)) = \alpha^{-1}(\alpha(A) \cap \alpha(B))$, uma vez que, claramente, $\alpha^{-1}(\alpha(X)) = X + Ker(\alpha)$ e

$\alpha^{-1}(X \cap Y) = \alpha^{-1}(X) \cap \alpha^{-1}(Y)$, para todo homomorfismo α e para todos X, Y submódulos de M. Logo $\alpha(A \cap B) = \alpha(\alpha^{-1}(\alpha(A \cap B))) = \alpha(\alpha^{-1}(\alpha(A) \cap \alpha(B))) = [\alpha(A) \cap \alpha(B)] \cap Im(\alpha) = \alpha(A) \cap \alpha(B)$.

$(iii) \Rightarrow (i)$ Sejam $A, B, C \in \mathcal{L}(M)$ submódulos quaisquer. Suponhamos que (iii) vale e consideremos $Q = M/C$. Definimos $\alpha : M \longrightarrow M/C$ por $\alpha(m) = m + C$, para todo $m \in M$. Segue que $C + (A \cap B) = \alpha(A \cap B) = \alpha(A) \cap \alpha(B) = (C + A) \cap (C + B)$. Logo M é um módulo distributivo. $\square$

Teorema 3.17. *Sejam P e Q módulos e $\alpha, \beta \in Hom(P, Q)$.*

(i) *Suponhamos que Q é um módulo distributivo e $X \subseteq P$ é um submódulo. Então :*

(a) $P = \beta^{-1}(Im(\alpha)) + \alpha^{-1}(Im(\beta))$.

(b) $X = (X \cap \beta^{-1}(\alpha(X))) + (X \cap \alpha^{-1}(\beta(X)))$.

(ii) *Suponha que P é um módulo distributivo e $X \subseteq Q$ é um submódulo. Então:*

(a) $0 = \beta((Ker(\alpha)) \cap \alpha(Ker(\beta))$.

(b) $X = (X + \beta(\alpha^{-1}(X))) \cap (X + \alpha(\beta^{-1}(X)))$.

Demonstração:

(i)

(a) Suponhamos que Q é um módulo distributivo, $X \subseteq P$ é um submódulo e $\alpha, \beta \in Hom(P, Q)$. Obsevemos inicialmente que $P = (\alpha+\beta)^{-1}(Im(\alpha) + Im(\beta))$. De fato, seja $p \in P$. Então $(\alpha+\beta)(p) = \alpha(p)+\beta(p) \in Im(\alpha)+Im(\beta)$. Segue que $p \in (\alpha + \beta)^{-1}((\alpha + \beta)(p)) = (\alpha + \beta)^{-1}(\alpha(p) + \beta(p)) \subseteq (\alpha + \beta)^{-1}(Im(\alpha) + Im(\beta))$. A outra contenção é óbvia e com isso mostramos a observação. Pelo fato de Q ser um módulo distributivo, o Lema 3.16 nos garante que $P = (\alpha + \beta)^{-1}(Im(\alpha) + Im(\beta)) = (\alpha + \beta)^{-1}(Im(\alpha)) +$

$(\alpha+\beta)^{-1}(Im(\beta))$. Para finalizar a demonstração basta mostrar que $(\alpha+\beta)^{-1}(Im(\alpha)) = \beta^{-1}(Im(\alpha))$. Para tanto, consideremos $x \in (\alpha+\beta)^{-1}(Im(\alpha))$. Então $\beta(x) \in Im(\alpha)$, com $x \in P$. Notemos também que $\alpha(x) \in Im(\alpha)$. Segue que $(\beta+\alpha)(x) = \beta(x)+\alpha(x) \in Im(\alpha)$ e isto implica que $x \in \beta^{-1}(Im(\alpha))$. Portanto $(\alpha+\beta)^{-1}(Im(\alpha)) \supseteq \beta^{-1}(Im(\alpha))$. Seja agora $x \in (\alpha+\beta)^{-1}(Im(\alpha))$. Então $\alpha(x)+\beta(x) = (\alpha+\beta)(x) \in Im(\alpha)$. Conseqüentemente $\beta(x) \in Im(\alpha)$, isto é, $x \in \beta^{-1}(Im(\alpha))$ e a afirmação está verificada. Com a primeira e a segunda afirmações obtemos: $P = (\alpha+\beta)^{-1}(Im(\alpha)+Im(\beta)) = (\alpha+\beta)^{-1}(Im(\alpha))+(\alpha+\beta)^{-1}(Im(\beta)) = \beta^{-1}(Im(\alpha))+\alpha^{-1}(Im(\beta))$.

(b) Suponhamos que Q é um módulo distributivo, $X \subseteq P$ é um submódulo e $\alpha, \beta \in Hom(P,Q)$. Seja i o homomorfismo $i : X \longrightarrow P$ dada por $i(x) = x$ para todo $x \in X$ (inclusão natural). Consideremos agora os homomorfismos $\alpha \circ i$, $\beta \circ i$ e aplicamos o ítem (i)(a) deste teorema para obter: $X = (\beta \circ i)^{-1}(Im(\alpha \circ i) + (\alpha \circ i)^{-1}(Im(\beta))$. Afirmamos que $(\beta \circ i)^{-1}(Im(\alpha \circ i)) = X \cap \beta^{-1}(\alpha(X))$. De fato $(\beta \circ i)^{-1}(Im(\alpha \circ i)) = i^{-1}(\beta^{-1}(\alpha(x))) = \beta^{-1}(\alpha(X)) \cap X$, pois i é a inclusão natural (vide Lema 3.16 $(ii) \Rightarrow (i)$). Logo $X = (\beta \circ i)^{-1}(Im(\alpha \circ i)) + (\alpha \circ i)^{-1}(Im(\beta)) = (X \cap \beta^{-1}(\alpha(X))) + (X \cap \alpha^{-1}(\beta(X)))$.

(ii)

(a) Suponhamos que P é um módulo distributivo, $X \subseteq Q$ é um submódulo e $\alpha, \beta \in Hom(P,Q)$. Daí,

$0 = (\alpha+\beta)(Ker(\alpha) \cap Ker(\beta)) = (\alpha+\beta)(Ker(\alpha)) \cap (\alpha+\beta)(Ker(\beta)) = \beta((Ker(\alpha)) \cap \alpha(Ker(\beta))$, onde a penúltima igualdade é garantida pelo Lema 3.16 (iii).

(b) Suponhamos que P é um módulo distributivo, $X \subseteq Q$ é um submódulo e $\alpha, \beta \in Hom(P,Q)$. Consideremos o homomorfismo $\pi : Q \longrightarrow Q/X$ dado por $\pi(x) = x + X$ para todo $x \in Q$ e os homomorfismos $\pi \circ \alpha$ e $\pi \circ \beta$.

Usando o ítem $(ii)(a)$ deste teorema obtemos:

$\overline{0} = X = (\pi \circ \beta)(Ker(\pi \circ \alpha)) \cap (\pi \circ \alpha)(Ker(\pi \circ \beta))$. Afirmamos que $(\pi \circ \beta)(Ker(\pi \circ \alpha)) = X + \beta(\alpha^{-1}(X))$. De fato, notemos que $Ker(\pi \circ \alpha) = \{x \in P \, : \, \alpha(x) \in X \text{ , } \textit{isto é, } x \in \alpha^{-1}(x)\}$. Portanto $Ker(\pi \circ \alpha) = \alpha^{-1}(X)$ e segue que $(\pi \circ \beta)(Ker(\pi \circ \alpha)) = (\pi \circ \beta)(\alpha^{-1}(X)) = \beta(\alpha^{-1}(X)) + X$. Segue daí que $X = (\pi \circ \beta)(Ker(\pi \circ \alpha)) \cap (\pi \circ \alpha)(Ker(\pi \circ \beta)) = (X + \beta(\alpha^{-1}(X))) \cap (X + \alpha(\beta^{-1}(X)))$. □

O próximo teorema nos fornece outra caracterização de módulos distributivos, porém esta, ao nível de elementos. Este resultado é muito útil para se fazer cálculos em anéis e módulos distributivos.

Teorema 3.18. *Para um R-módulo à direita as seguintes sentenças são equivalentes:*

(i) *M é um módulo distributivo.*

(ii) $(aR : b) + (bR : a) = R$*, para todo* $a, b \in M$.

(iii) $(a + b)R = (aR \cap (a + b)R) + (bR \cap (a + b)R)$*, para todo* $a, b \in M$.

(iv) $aR + bR = (a + b)R + (aR \cap bR)$*, para todo* $a, b \in M$.

Demonstração:

$(i) \Rightarrow (ii)$ Tomando $P = R$, $Q = M$ e definindo os homomorfismos $\alpha : R \longrightarrow M$, por $\alpha(1) = a$, e $\beta : R \longrightarrow M$, por $\beta(1) = b$, ficamos nas hipóteses do Teorema 3.17. Segue daí que $R = \beta^{-1}(Im(\alpha)) + \alpha^{-1}(Im(\beta)) = \beta^{-1}(aR) + \alpha^{-1}(bR) = (aR : b) + (bR : a)$ e a implicação está provada.

$(ii) \Rightarrow (iii)$ Temos, por hipótese, que $(a + b)R = (a + b)[(aR : b) + (bR : a)] = (aR \cap (a+b)R) + (bR \cap (a+b)R)$, onde provaremos a última igualdade. De fato, seja $x \in (a + b)[(aR : b) + (bR : a)]$. Então $x = (a + b).(r_1 + r_2)$ onde $br_1 \in aR$ e $ar_2 \in bR$. Distribuindo obtemos $x = y_1 + y_2$ com $y_1 \in$

$aR \cap (a+b)R$ e $y_2 \in bR \cap (a+b)R$. Para verificar a outra contenção, mostraremos que $aR \cap (a+b)R = (a+b)(aR : (a+b))$. Para tanto consideremos $x \in aR \cap (a+b)R$. Então $x = ar_1 = (a+b)r_2 \in (a+b)(aR : (a+b))$. Portanto $aR \cap (a+b)R \subseteq (a+b)(aR : (a+b))$. Observemos que a contenção $aR \cap (a+b)R \supseteq (a+b)(aR : (a+b))$ é imediata, pois um elemento de $(a+b)(aR : (a+b))$ é da forma $(a+b)x$, pertencente à $(a+b)R$ e à aR.

$(iii) \Rightarrow (i)$ Sejam $A, B, C \in \mathcal{L}(M)$ e suponhamos que $c = a + b \in (C \cap (A+B))$, onde $a \in A$, $b \in B$ e $c \in C$. Segue, por (iii), que $cR = (a+b)R = (aR \cap (a+b)R) + (bR \cap (a+b)R) = (aR \cap cR) + (bR \cap cR)$. Então $c \in (C \cap A) + (C \cap B)$. Portanto $C \cap (A+B) \subseteq (C \cap A) + (C \cap B)$. Como a outra inclusão sempre é válida, temos $C \cap (A+B) = (C \cap A) + (C \cap B)$, isto é, M é distributivo.

$(iv) \Rightarrow (ii)$ Suponhamos (iv) válida. Então $aR = aR \cap (aR + bR) = aR \cap ((a+b)R + (aR \cap bR)) = (aR \cap (a+b)R) + (aR \cap bR)$, onde a última igualdade é facilmente verificada. Usando que $aR \cap (a+b)R = (a+b)(aR : (a+b))$, mostrado anteriormente, obtemos: $aR = (aR \cap (a+b)R) + (aR \cap bR) = (a+b)(aR : (a+b)) + (aR \cap bR) = (a+b)(aR : b) + (aR \cap bR)$. Consideremos agora $x \in ((a+b)(aR : b) + (aR \cap bR))$. Então $x = (a+b)c + y$, onde $c \in (aR : b)$ e $y \in aR \cap bR$. Daí $x = ac + bc + y = ac + (bc + y) \in a(aR : b) + (aR \cap bR)$. Reciprocamente, seja $x' \in a(aR : b) + (aR \cap bR)$. Então existem $c' \in (aR : b)$ e $y' \in aR \cap bR$ tais que $x' = ac' + y' = ac' + bc' - bc' + y' = (a+b)c' + (-bc' + y') \in ((a+b)(aR : b) + (aR \cap bR))$. Logo, $(a+b)(aR : b) + (aR \cap bR) = a(aR : b) + (aR \cap bR)$. Assim temos $aR = a(aR : b) + (aR \cap bR) = a(aR : b) + a(bR : a)$, pois trivialmente $a(bR : a) = aR \cap bR$. Segue que $aR = a(aR : b) + a(bR : a)$ e isto implica que $a[R - ((aR : b) + (bR : a))] = 0$. Observemos que $r(a) \subseteq (bR : a)$. Conseqüentemente $R - ((aR : b) + (bR : a)) = 0$, isto é, $R = (aR : b) + (bR : a)$.

$(i) \Rightarrow (iv)$ Suponhamos que M é um módulo distributivo. Começamos afirmando que $aR + bR = bR + (a+b)R$, para todo $a, b \in M$. De fato, seja $x \in aR + bR$, então existem $r_1, r_2 \in R$, tais que $x = ar_1 + br_2 = ar_1 + br_1 - br_1 + br_2 = (a+b)r_1 + b(r_2 - r_1) \in (a+b)R + bR$. A outra contenção é imediata. Com isso temos $aR \subseteq aR + bR = bR + (a+b)R$. Segue que $aR = aR \cap (bR + (a+b)R)$. Como M é um módulo distributivo obtemos $aR = aR \cap bR + aR \cap (a+b)R$. Similarmente temos $bR = aR \cap bR + bR \cap (a+b)R$. Somando as duas igualdades temos $aR + bR = aR \cap bR + aR \cap (a+b)R + bR \cap (a+b)R = (aR + bR) \cap (a+b)R + aR \cap bR = (a+b)R + aR \cap bR$, pois $aR + bR \supseteq (a+b)R$. Logo $aR + bR = (a+b)R + (aR \cap bR)$. □

Abaixo, vemos um exemplo de módulo distributivo.

Exemplo 3.19. O anel $\mathbb{Q}$, tomado como um $\mathbb{Z}$-módulo é distributivo.

De fato pois, como $\mathbb{Z}$ é um anel distributivo, mostrado no Exemplo 1.25 segue, pelo Teorema 3.18 que, para todo $a, b \in \mathbb{Z}$, $(aR : b) + (bR : a) = \mathbb{Z}$. Dados $x, y \in \mathbb{Q}$, podemos escrever $x = a's^{-1}$ e $y = b's^{-1}$ com $a', b' \in \mathbb{Z}$ e $s \in S = \mathbb{Z} \backslash \{0\}$. Além disso, claramente $(a'R : b') = (a's^{-1}R : b's^{-1})$ para todo $s \in S = \mathbb{Z} \backslash \{0\}$. Conseqüentemente $(a's^{-1}R : b's^{-1}) + (b's^{-1}R : a's^{-1}) = \mathbb{Z}$. Logo, novamente pelo Teorema 3.18 , temos que $\mathbb{Q}$ é um $\mathbb{Z}$-módulo distributivo. □

Corolário 3.20. *Suponhamos que M é um R-módulo distributivo e que $a, b \in M$.*

(i) Se $aR \cap bR = 0$, então $aR + bR = (a+b)R$ e $r(a) + r(b) = R$.

(ii) Se $r(a) \subseteq J(R)$, então aR é um submódulo essencial de M.

Demonstração:

(i) Suponhamos que M é um R-módulo distributivo. Sejam $a, b \in M$ tais que $aR \cap bR = 0$. Pelo ítem (iv) do Teorema 3.18 $aR + bR = (a + b)R + aR \cap bR = (a + b)R$. Observemos agora que $r(b) = (aR : b)$, uma vez que $aR \cap bR = 0$. Segue, usando o ítem (ii) do Teorema 3.18 que $R = (aR : b) + (bR : a) = r(b) + r(a)$. Logo $aR + bR = (a + b)R$ e $r(a) + r(b) = R$.

(ii)Suponhamos que M é um R-módulo distributivo. Seja $a \in M$ tal que $r(a) \subseteq J(R)$. Suponhamos que existe $b \in M$ tal que $aR \cap bR = 0$. Devemos mostrar que $bR = 0$. Para tanto lembremos que o ítem (i) deste corolário nos diz que $r(b) + r(a) = R$. Como $r(a) \subseteq J(R)$ e $r(b) + r(a) = R$, segue que $r(b) = R$ e conseqüentemente $b = 0$. Logo aR é um submódulo essencial. $\square$

3.2 Aplicações em anéis distributivos à direita

Começaremos esta seção com um exemplo dado por Mazurek em [12] de um anel distributivo que não é de cadeia e cujo radical de Jacobson é completamente primo.

Exemplo 3.21. Seja R o anel de todas as matrizes da forma $\begin{bmatrix} z & q \\ 0 & z \end{bmatrix}$, onde $z \in \mathbb{Z}$ e $q \in \mathbb{Q}$, com as operações usuais de matrizes. Então R é um anel comutativo. Obsevemos que o conjunto

$K = \left\{ \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix} \in R \,|\, q \in \mathbb{Q} \right\}$ é um ideal bilateral de R. Claramente temos $R/K \simeq \mathbb{Z}$, de onde segue que K é um ideal completamente primo. Além disso, como $\mathbb{Z}$, é distributivo, mostrado no Exemplo 1.25, temos que R/K também é distributivo. Considerando agora $\mathbb{Q}$ como um $\mathbb{Z}$-módulo, temos, pelo Exemplo 3.19, que o reticulado dos submódulos de $\mathbb{Q}$ é distributivo, o que nos leva a concluir que o reticulado dos ideais de R abaixo de K é distributivo, uma vez que são isomorfos ao reticulado dos $\mathbb{Z}$-submódulos de $\mathbb{Q}$. Além disso, facilmente vemos que $I \subseteq K$ ou $K \subseteq I$, para qualquer ideal I de R. Logo R é um anel distributivo.

Notemos também que $J(R) = K$. De fato pois, os ideais maximais de R são da forma $\left\{ \begin{bmatrix} p\mathbb{Z} & \mathbb{Q} \\ 0 & p\mathbb{Z} \end{bmatrix} \mid p \in \mathbb{Z}, p\, primo \right\}$ uma vez que se $I \nsubseteq K$ então $K \subseteq I$, $R/K \simeq \mathbb{Z}$ e os ideais maximais de $\mathbb{Z}$ são gerados pelos elementos primos.

Observemos ainda que este anel não é um anel de cadeia pois, tomando $I_1 = \left\{ \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix} \mid q \in (1/2)\mathbb{Z} \right\}$ e $I_2 \left\{ \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix} \mid q \in (1/3)\mathbb{Z} \right\}$ temos $I_1 \nsubseteq I_2$ e $I_2 \nsubseteq I_1$. $\square$

No exemplo acima, $J(R) = K$ é um ideal completamente primo tal que $I \subseteq K$ ou $K \subseteq I$, para qualquer ideal I de R. Observemos que isto é um fato geral, como será mostrado na próxima proposição.

Lembremos ainda que um anel é distributivo à direita se o módulo R_R à direita é distributivo.

Proposição 3.22. *Suponha que R é um anel distributivo à direita e P, Q são ideais à direita de R completamente primos. Então:*

(i) $P \subseteq Q$ ou $Q \subseteq P$ ou $P + Q = R$.

(ii) Se $P \subseteq J(R)$, então $I \subseteq P$ ou $P \subseteq I$, para qualquer ideal à direita I de R.

Demonstração:

(i) Suponhamos que $P \nsubseteq Q$ e $Q \nsubseteq P$. Então existe $p \in P$ e $q \in Q$ tal que $p \notin Q$ e $q \notin P$. Pelo Teorema 3.18 (ii) temos que $(pR : q) + (pR : q) = R$. Afirmamos que $(pR : q) \subseteq P$ e $(qR : p) \subseteq Q$. De fato, consideremos $x \in (pR : q)$. Então $qx \in pR$ e conseqüentemente $qx \in P$. Como $q \notin P$ e P é um ideal completamente primo de R, temos $x \in P$. Portanto $(pR : q) \subseteq P$ e analogamente $(qR : p) \subseteq Q$. Com isso $R \supseteq P + Q \supseteq (pR : q) + (pR : q) = R$.

Logo $P + Q = R$.

(ii) Suponhamos $P \subseteq J(R)$ e seja I um ideal à direita de R tal que $I \nsubseteq P$. Então existe $a \in I$ tal que $a \notin P$. O Teorema 3.18 (ii) nos garante que para todo $p \in P$ vale $(aR : p) + (pR : a) = R$. Agora, como $(pR : a) \subseteq P$, para todo $p \in P$, pelo mesmos raciocínio feito no ítem (i), segue que $(aR : p) = R$, uma vez que $R = (aR : p) + P$ e $P \subseteq J(R)$. Logo $pR \subseteq aR \subseteq I$, para todo $p \in P$, e o resultado segue. □

Proposição 3.23. *Sejam P e Q módulos e $\alpha, \beta \in Hom(P, Q)$.*

(i) *Se Q é um módulo à direita distributivo, então $Im(\alpha) \cap Im(\beta) = 0$ implica que $Ker(\alpha) + Ker(\beta) = P$.*

(ii) *Se P é um módulo à direita distributivo, então $Ker(\alpha) + Ker(\beta) = P$ implica que $Im(\alpha) \cap Im(\beta) = 0$.*

(iii) *Se P e Q são módulos distributivos à direita e $Im(\alpha) \cap Im(\beta) = 0$, então:*

$$Im(\alpha + \beta) = Im(\alpha) + Im(\beta) \text{ e } Ker(\alpha + \beta) = Ker(\alpha) \cap Ker(\beta).$$

Demonstração:

(i) Suponhamos que Q é um módulo distributivo. Sabemos, do Teorema 3.17 (i) que $P = \beta^{-1}(Im(\alpha)) + \alpha^{-1}(Im(\beta))$. Observemos que se $Im(\alpha) \cap Im(\beta) = 0$ então $\beta^{-1}(Im(\alpha)) = Ker(\beta)$. De fato, seja $x \in P$ tal que $\beta(x) \in Im(\alpha)$. Segue que $\beta(x) = 0$ e isto implica que $x \in Ker(\beta)$. Portanto $\beta^{-1}(Im(\alpha)) \subseteq Ker(\beta)$. A outra contenção é óbvia. Analogamente $\alpha^{-1}(Im(\beta)) = Ker(\alpha)$. Portanto temos $P = \beta^{-1}(Im(\alpha)) + \alpha^{-1}(Im(\beta)) = Ker(\beta) + Ker(\alpha)$.

(ii) Suponhamos que P é um módulo distributivo e $Ker(\alpha) + Ker(\beta) = P$. O Teorema 3.17 (ii) nos diz que $0 = \beta(Ker(\alpha)) \cap \alpha(Ker(\beta))$. Para concluir a demonstração basta mostrar que $\beta(Ker(\alpha)) = Im(\beta)$ e $\alpha(Ker(\beta)) = Im(\alpha)$. Obviamente $\beta(Ker(\alpha)) \subseteq Im(\beta)$. Para verificar a outra contenção, consideremos $x \in Im(\beta)$. Então existe $x' \in P$ tal que $\beta(x') = x$. Como $Ker(\alpha) + Ker(\beta) = P$, podemos escrever $x' = x_\alpha + x_\beta$ com $x_\alpha \in Ker(\alpha)$ e $x_\beta \in Ker(\beta)$. Segue que $x = \beta(x') = \beta(x_\alpha + x_\beta) = \beta(x_\alpha) + \beta(x_\beta) = \beta(x_\alpha) \in \beta(Ker(\alpha))$. Portanto $\beta(Ker(\alpha)) = Im(\beta)$. Analogamente $\alpha(Ker(\beta)) = Im(\alpha)$.

(iii) Suponhamos que P e Q são módulos distributivos e $Im(\alpha) \cap Im(\beta) = 0$. Inicialmente mostraremos que se $Im(\alpha) \cap Im(\beta) = 0$ então $Ker(\alpha + \beta) = Ker(\alpha) \cap Ker(\beta)$. De fato, pois obviamente $Ker(\alpha + \beta) \supseteq Ker(\alpha) \cap Ker(\beta)$. Para mostrar a outra contenção consideremos $x \in Ker(\alpha + \beta)$. Então $0 = (\alpha + \beta)(x) = \alpha(x) + \beta(x)$ e isto implica que $\alpha(x) = -\beta(x)$. Como $Im(\alpha) \cap Im(\beta) = 0$ temos $\alpha(x) = -\beta(x) = 0$. Portanto $x \in Ker(\alpha)$ e $x \in Ker(\beta)$. Logo, $Ker(\alpha + \beta) = Ker(\alpha) \cap Ker(\beta)$. Para verificar que $Im(\alpha+\beta) = Im(\alpha)+Im(\beta)$ observemos que, por (i) e (ii), $Im(\alpha) \cap Im(\beta) = 0$ ocorre se, e somente se, $Ker(\alpha) + Ker(\beta) = P$. Portanto $Im(\alpha) + Im(\beta) = \beta(Ker(\alpha)) + \alpha((Ker(\beta)) = (\alpha + \beta)(Ker(\alpha)) + (\alpha + \beta)(Ker(\beta)) = (\alpha + \beta)(Ker(\alpha) + Ker(\beta)) = (\alpha + \beta)(P) = Im(\alpha + \beta)$. □

A implicação ($\Rightarrow$) do próximo resultado já foi provada no Corolário 3.20. Porém daremos uma prova alternativa, usando a proposição anterior.

Corolário 3.24. *Suponhamos que R é um anel distributivo à direita e Q é um R-módulo distributivo com $a, b \in Q$. Então $aR \cap bR = 0$ se, e somente se, $r(a) + r(b) = R$.*

Demonstração:

Suponhamos que R é um anel distributivo à direita e Q é um R-módulo à direita distributivo com $a, b \in Q$, tais que $aR \cap bR = 0$. Definimos os homomorfismos $\alpha : R \longrightarrow Q$ por $\alpha(x) = ax$, para todo $x \in R$ e $\beta : R \longrightarrow Q$

por $\beta(x) = bx$, para todo $x \in R$. Fazendo $P = R$ nos ítens (i) e (ii) da proposição anterior, segue que $Im(\alpha) \cap Im(\beta) = 0$. Pelo ítem (i) da proposição anterior isto implica que $Ker(\alpha) + Ker(\beta) = R$. Da maneira que definimos α e β obtemos $Ker(\alpha) = r(a)$ e $Ker(\beta) = r(b)$, ou seja, $r(a)+r(b) = R$. A recíproca segue direto do ítem (ii) da proposição anterior. $\square$

Lembremos que dados R um anel, M um R-módulo à direita e P um submódulo, P é chamado de *submódulo inessencial* de M se $P + Q \neq M$, para todo $Q \in \mathcal{L}(M)$, com $Q \neq M$.

Proposição 3.25. *Sejam P e Q módulos e $\alpha, \beta \in Hom(P, Q)$.*

(i) *Suponhamos que todo submódulo próprio de P é inessencial e Q é um módulo distributivo. Então $Im(\alpha) \subseteq Im(\beta)$ ou $Im(\alpha) \supseteq Im(\beta)$.*

(ii) *Suponhamos que todo submódulo próprio de Q é essencial (isto é, Q é um módulo uniforme) e P é um módulo distributivo. Então $Ker(\alpha) \subseteq Ker(\beta)$ ou $Ker(\alpha) \supseteq Ker(\beta)$.*

Demonstração:

(i) Suponhamos que todo submódulo próprio de P é inessencial e Q é um módulo distributivo. Pelo Teorema 3.17 (i) $P = \beta^{-1}(Im(\alpha)) + \alpha^{-1}(Im(\beta))$. Como P é inessencial, temos $\beta^{-1}(Im(\alpha)) = P$ ou $\alpha^{-1}(Im(\beta)) = P$. Afirmamos que $\beta^{-1}(Im(\alpha)) = P$ implica $Im(\beta) \subseteq Im(\alpha)$. De fato, se por absurdo ocorresse $Im(\beta) \nsubseteq Im(\alpha)$, existiria $x' \in P$ tal que $\beta(x') \notin Im(\alpha)$. Conseqüentemente teríamos que $x' \notin \beta^{-1}(Im(\alpha))$ o que é um absurdo pois $\beta^{-1}(Im(\alpha)) = P$. Analogamente, $\alpha^{-1}(Im(\beta)) = P$ implica $Im(\alpha) \subseteq (Im(\beta))$. Logo $Im(\alpha) \subseteq Im(\beta)$ ou $Im(\alpha) \supseteq Im(\beta)$.

(ii) Suponhamos que todo submódulo próprio de Q é essencial e P é um módulo distributivo. Pelo Teorema 3.17 (ii) temos $0 = (\beta(Ker(\alpha))) \cap (\alpha(Ker(\beta)))$. Como Q é essencial temos que $\beta(Ker(\alpha)) = 0$ ou $\alpha(Ker(\beta)) = 0$. Segue que $Ker(\alpha) \subseteq Ker(\beta)$ ou $Ker(\beta) \subseteq Ker(\alpha)$. $\square$

Corolário 3.26. *Se R é um anel local, e Q é um R-módulo distributivo, então os submódulos de Q são totalmente ordenados.*

Demonstração:

Sejam R é um anel local, Q um R-módulo distributivo e $a, b \in Q$. Começamos observando que se R é um anel local, então todo ideal P de R é inessencial pois dado P maximal, não existe um ideal I de R tal que $P + I = R$. Definimos os homomorfismos $\alpha : R \longrightarrow Q$, por $\alpha(1) = a$, e $\beta : R \longrightarrow Q$, por $\beta(1) = b$, onde $\alpha, \beta \in Hom(R_R, Q)$. Pelo ítem (i) da proposição acima temos $Im(\alpha) \subseteq Im(\beta)$ ou $Im(\alpha) \supseteq Im(\beta)$. Neste caso $aR \subseteq bR$ ou $bR \subseteq aR$. Daí segue que os submódulos de Q são totalmente ordenados. $\square$

Como uma consequência imediata do resultado acima, reobtemos (vide Proposição 2.6) o resultado do corolário abaixo usando outros argumentos.

Corolário 3.27. *Seja R um anel distributivo à direita. Então R é local se, e somente se, R é um anel de cadeia à direita.*

Corolário 3.28. *Suponhamos que R é um anel distributivo à direita e Q é um R-módulo distributivo. Então Q é uniforme se, e somente se, os anuladores à direita dos elementos de Q são totalmente ordenados.*

Demonstração:

Sejam R um anel distributivo à direita, Q um R-módulo distributivo e $a, b \in Q$. Suponhamos que Q é uniforme. Tomemos $a, b \in Q$ quaisquer. Definimos $\alpha : R \longrightarrow Q$ por $\alpha(1) = a$ e $\beta : R \longrightarrow Q$ por $\beta(1) = b$. Considerando $P = R$ na Proposição 3.25 (ii) obtemos $Ker(\alpha) \subseteq Ker(\beta)$ ou

$Ker(\beta) \subseteq Ker(\alpha)$, que neste caso a dizer que $r(a) \subseteq r(b)$ ou $r(b) \subseteq r(a)$. Portanto os anuladores à direita dos elementos de Q são totalmente ordenados. Reciprocamente, suponhamos que os anuladores à direita dos elementos de Q são totalmente ordenados. Sejam $c, d \in Q$ quaisquer e suponhamos que $cR \cap dR = 0$. Devemos mostrar que $cR = 0$ ou $dR = 0$. O Corolário 3.24 nos afirma que $cR \cap dR = 0$ se, e somente se, $r(c) + r(d) = R$. Como os anuladores são totalmente ordenados vale $r(c) \subseteq r(b) = R$ ou $r(d) \subseteq r(c) = R$, como queríamos mostrar. $\square$

Para o próximo corolário necessitamos do seguinte lema, cuja prova é direta e não será apresentada aqui.

Lema 3.29. *Sejam A, B ideais à direita de um anel arbritário R.*

(i) Se $A \subseteq B$ então $l(B) \subseteq l(A)$ e $r(B) \subseteq r(A)$.

(ii) $A \subseteq r(l(A))$.

(iii) $l(A) = l(r(l(A)))$. $\square$

Corolário 3.30. *Suponhamos que R é um anel distributivo. Então R é uniforme à direita se, e somente se, R é uniforme à esquerda.*

Demonstração:

Suponhamos que R é um R-módulo à direita uniforme. Pelo corolário anterior segue que $\{r(a)\}_{a \in R}$ é linearmente ordenado por inclusão e isto ocorre se, e somente se, os anuladores à direita dos subconjuntos de R são linearmente ordenados por inclusão pois, se $S \subseteq R$, então $r(S) = \bigcap_{s \in S} r(s)$. Tomemos agora $x, y \in R$. Pelo ítem (iii) do lema anterior $l(x) = l(r(l(x)))$ e $l(y) = l(r(l(y)))$. Como $l(x)$ e $l(y)$ são subconjuntos de R temos $r(l(x)) \subseteq r(l(y))$ ou $r(l(y)) \subseteq r(l(x))$. Suponhamos $r(l(x)) \subseteq r(l(y))$. Segue, pelo ítem (i) do lema anterior que $l(r(l(y))) \subseteq l(r(l(x)))$. Usando novamente o ítem (iii)

do lema anterior obtemos $l(y) \subseteq l(x)$. Portanto $\{l(a)\}_{a \in R}$ é uma família totalmente ordenada e, pelo corolário anterior, R é uniforme à esquerda. A recíproca é análoga. $\square$

Capítulo 4

O Reticulado de Submódulos Saturados em Anéis e Módulos Distributivos à Direita

Trataremos neste capítulo sobre submódulos saturados em anéis e módulos à direita, seguindo o trabalho de Ferrero e Sant'Ana [7], abrangendo as seções 2, 3 e 4.

Usaremos notação $Max(R)$ para indicar o conjunto de todos ideais maximais de R e a notação $S_P = R \backslash P$ onde $P \in Max(R)$.

4.1 Caracterização da Distributividade por Submódulos Saturados.

Começamos relembrando que um submódulo N de um R-módulo M é dito S-saturado se $NS^{-1} = N$, onde $S \subseteq R$ é um subconjunto multiplicamente fechado (Definição 1.20).

Vamos agora a um lema que nos dará um resultado muito útil para o que se segue.

Lema 4.1. *Sejam S um conjunto de Ore à direita e N um submódulo de M. Então NS^{-1} é um submódulo S-saturado de M.*

Demonstração:

Primeiramente verifiquemos que NS^{-1} é um submódulo de M. Para tanto consideremos $x, y \in NS^{-1}$. Então $xs \in N$ e $yt \in N$, para certos $s, t \in S$. Como S é um conjunto de Ore à direita, existem $a, b \in S$ tais que $sa = tb = u \in S$. Segue que $(x+y)u = xu+yu = xsa+ytb \in N$. Portanto $x+y \in NS^{-1}$. Sejam agora $x \in NS^{-1}$. Então existe $s \in S$ tal que $xs \in N$. Consideremos $a \in R$. Afirmamos que $xa \in NS^{-1}$. De fato, pois como S é um conjunto de Ore à direita, existem $b \in R$ e $t \in S$ tais que $at = sb$. Usando o fato de N ser um submódulo obtemos $N \ni (xs)b = x(sb) = x(at) = (xa)t$, o que implica que $xa \in NS^{-1}$, uma vez que $t \in S$. Portanto NS^{-1} é um submódulo de M. Provemos agora que NS^{-1} é S-saturado, isto é, $(NS^{-1})S^{-1} = NS^{-1}$. Obviamente $(NS^{-1})S^{-1} \supseteq NS^{-1}$. Seja $x \in (NS^{-1})S^{-1}$. Então existe $s_1 \in S$ tal que $xs_1 \in NS^{-1}$. Mas $xs_1 \in NS^{-1}$ implica que existe $s_2 \in S$ tal que $xs_1s_2 \in N$. Como S é multiplicativamente fechado, $s_1s_2 \in S$ e segue que $x \in NS^{-1}$. $\square$

Observemos que a última etapa do lema acima é uma generalização do Corolário 2.16.

Definição 4.2. *Seja R um anel. R é dito um anel admissível à direita se para todo $P \in Max(R)$, $S_P = R\backslash P$ é um conjunto de Ore à direita.*

Proposição 4.3. *Seja M um R-módulo. Então M é distributivo se, e somente se, para todo $x, y \in M$ e $P \in Max(R)$, existe $s \in S_p$ tal que $xs \in yR$*

ou $ys \in xR$.

Demonstração: Suponhamos que M é distributivo. Então segue do Teorema 3.18 que $(xR : y) + (yR : x) = R$. Assim, existem $s, t \in R$ com $s \in (xR : y)$ e $t \in (yR : x)$, tais que $s + t = 1$. Segue que $ys \in xR$ e $xt \in yR$ com $s \in S_P$ ou $t \in S_P$, pois se $s, t \in P$ teríamos que $1 = s+t \in P$, o que é um absurdo. Reciprocamente, suponhamos que, para todo $P \in Max(R)$, existe $s \in S_P$ com $xs \in yR$ ou $ys \in xR$. Consideremos $(yR : x) + (xR : y) = A$. Suponhamos $A \neq R$ e tomemos P maximal tal que $A \subseteq P$ e, sem perda de generalidade, suponhamos que $xs \in yR$, onde $s \in S_P$. Conseqüentemente $s \in (yR : x) \cap S_P \subseteq A \cap S_P$ e isto é uma contradição pois $A \cap S_P = 0$, uma vez que $S_P = R \backslash P$ e $A \subseteq P$. Logo $(xR : y) + (yR : x) = R$ e pelo Teorema 3.18, M é um módulo distributivo. $\square$

Notemos que se R é um anel distributivo à direita, então qualquer ideal maximal à direita P de R é um ideal bilateral, completamente primo e S_P é um conjunto de Ore à direita. Portanto R é admissível. De fato pois, pela observação feita logo após o Corolário 1.15, se $P \in Max(R)$ então P é bilateral e completamente primo. Resta verificar que $S_P = R \backslash P$ é um conjunto de Ore. Porém, a proposição acima nos garante que, dados $x \in R$ e $y \in S$, existe $s \in S$ tal que $xs \in yR$ ou $ys \in xR$. Como S é multiplicativamente fechado, S é um conjunto de Ore.

Para demonstrar o próximo teorema, necessitamos dos seguintes lemas.

Lema 4.4. *Sejam R um anel admissível, M um R-módulo e N um submódulo de M. Então $N = \bigcap_{P \in Max(R)} N{S_P}^{-1}$.*

Demonstração:

Claramente $N \subseteq \bigcap_{P \in Max(M)} N{S_P}^{-1}$, uma vez que $N \subseteq N{S_P}^{-1}$, para todo $P \in Max(R)$. Para mostrar a outra contenção, consideremos $x \notin N$.

O ideal à direita $(N : x) = \{r \in R \mid xr \in N\}$ é um ideal à direita próprio e então existe $P \in Max(R)$ tal que $(N : x) \subseteq P$. Segue que, para todo $s \in S_P$, $xs \notin N$ e conseqüentemente $x \notin N{S_P}^{-1}$. Portanto $N{S_P}^{-1} \subseteq N$. Logo $N = \bigcap_{P \in Max(M)} N{S_P}^{-1}$. $\square$

Lema 4.5. *Sejam M um R-módulo, $P \in Max(R)$ e S_P um conjunto de Ore à direita. Para submódulos K e N de M temos $(K \cap N){S_P}^{-1} = K{S_P}^{-1} \cap N{S_P}^{-1}$.*

Demonstração:

Seja $x \in K{S_P}^{-1} \cap N{S_P}^{-1}$. Então existe $s, t \in S_P$ tal que $xs \in K$ e $xt \in N$. Também existem $u, v \in S_P$ com $su = tv$. Segue que $xsu = xtv \in K \cap N$ e conseqüentemente $x \in (K \cap N){S_P}^{-1}$. Com isso mostramos que $(K \cap N){S_P}^{-1} \supseteq K{S_P}^{-1} \cap N{S_P}^{-1}$. Para mostrar a outra contenção, consideremos $x \in (K \cap N){S_P}^{-1}$. Então existe $s \in S_P$ tal que $xs \in K \cap N$, isto é , existe $s \in S_P$ tal que $xs \in K$ e $xs \in N$. Isto implica que $x \in K{S_P}^{-1} \cap N{S_P}^{-1}$. Logo $(K \cap N){S_P}^{-1} = K{S_P}^{-1} \cap N{S_P}^{-1}$. $\square$

Teorema 4.6. *Sejam R um anel admissível à direita e M um R-módulo à direita. Então as seguintes condições são equivalentes:*

(i) M é distributivo.

(ii) Para qualquer $P \in Max(R)$ o reticulado dos submódulos S_P-saturados de M é linearmente ordenado por inclusão.

(iii) Para qualquer $P \in Max(R)$ o reticulado dos submódulos S_P-saturados de M é distributivo e fechado em relação à adição.

Demonstração:

$(i) \Rightarrow (ii)$ Sejam M distributivo e P um ideal maximal. Consideremos K

e N submódulos S_P-saturados, isto é , $K = KS_P{}^{-1}$ e $N = NS_P{}^{-1}$. Suponhamos que $N \nsubseteq K$ e tomemos $x \in N \backslash K$. Segue então da Proposição 4.3 que para cada $y \in K$, existe $s \in S_P$, tal que $ys \in xR \subseteq N$ ou $xs \in yR \subseteq K$. Se ocorrer $xs \in yR \subseteq K$, temos $x \in KS_P{}^{-1}$, o que é uma contradição. Portanto $ys \in xR \subseteq N = NS_P^{-1}$, de onde segue que $y \in N$. Logo $K \subseteq N$.

$(ii) \Rightarrow (iii)$ Suponhamos que para todo $P \in Max(R)$ o reticulado dos submódulos S_P-saturados de M é linearmente ordenado por inclusão. Então claramente este reticulado é fechado em relação à adição e distributivo.

$(iii) \Rightarrow (i)$ Para demonstrar essa implicação mostraremos inicialmente que para submódulos K e N de M e $P \in Max(R)$ temos $(K+N)S_P{}^{-1} = KS_P{}^{-1} + NS_P{}^{-1}$. De fato, segue do Lema 4.1 que $KS_P{}^{-1}$e $NS_P{}^{-1}$ são S_P-saturados. Notemos ainda que $K+N \subseteq KS_P{}^{-1}+NS_P{}^{-1}$. Com isso obtemos $(K+N)S_P{}^{-1} \subseteq (KS_P{}^{-1} + NS_P{}^{-1})S_P{}^{-1} = KS_P{}^{-1} + NS_P{}^{-1}$. Para a outra contenção consideremos $a \in KS_P^{-1} + NS_P^{-1}$. Então $a = x + y$ com $x \in KS_P^{-1}$ e $y \in NS_P^{-1}$. Segue que existem $s_1, s_2 \in S_P$ tais que $xs_1 \in K$ e $ys_2 \in N$. Como R é admissível, S_P é um conjunto de Ore à direita, então existem $t_1, t_2 \in S$ tais que $s_1t_1 = s_2t_2 = u \in S$. Temos ainda que $xs_1t_1 = xu \in K$ e $ys_2t_2 = yu \in N$, uma vez que K e N são submódulos à direita. Segue que $au = xu + yu = (x + y)u \in K + N$. Logo $a \in (K + S)S_P$.

Consideremos agora K, L, N submódulos de M. Aplicando o Lema 4.5 no resultado acima e usando a hipótese, obtemos, para todo $P \in Max(R)$:

$((K+L)\cap N)S_P{}^{-1} = (K+L)S_P{}^{-1}\cap NS_P{}^{-1} = (KS_P{}^{-1}+LS_P{}^{-1})\cap NS_P{}^{-1} = (KS_P{}^{-1} \cap NS_P{}^{-1}) + (LS_P{}^{-1} \cap NS_P{}^{-1}) = (K \cap N)S_P{}^{-1} + (L \cap N)S_P{}^{-1} = [(K \cap N) + (L \cap N)]S_P{}^{-1}$.

Pelo Lema 4.4 segue que $(K + L) \cap N = (K \cap N) + (L \cap N)$, isto é, M é distributivo. $\square$

Observemos agora que, se R é um anel qualquer e M é um R-módulo à direita distributivo que contém algum elemento z cujo anulador é o zero ($r(z) = 0$),então $R \simeq zR \subseteq M$. Conseqüentemente R também é distributivo à direita. Em vista disso, temos, de maneira imediata, o seguinte corolário:

Corolário 4.7. *Sejam R um anel e M um R-módulo à direita que contém algum elemento cujo anulador é o zero. Então as seguintes sentenças são equivalentes:*

(i) M é distributivo.

(ii) R é distributivo à direita e, para qualquer $P \in Max(R)$, o reticulado dos submódulos S_P-saturados de M é linearmente ordenado por inclusão.

(iii) R é admissível e, para qualquer $P \in Max(R)$, o reticulado dos submódulos S_P-saturados de M é distributivo e fechado em relação à adição.

Além disso, considerando o R-módulo R_R, o seguinte resultado fica evidente.

Corolário 4.8. *Seja R um anel. Então as seguintes sentenças são equivalentes:*

(i) R é distributivo à direita.

(ii) Para quaisquer $a, b \in R$ e qualquer $P \in Max(R)$ existe $s \notin P$ tal que $as \in bR$ ou $bs \in aR$.

(iii) R é admissível e para qualquer $P \in Max(R)$ o reticulado dos ideais à direita S_P-saturados de R é linearmente ordenado por inclusão.

(iv) R é um anel admissível e para qualquer $P \in Max(R)$ o reticulado dos ideais à direita de R é distributivo e fechado em relação à adição.

Em [17] Torner e Zima provaram o seguinte resultado para domínios distributivos à direita.

Lema 4.9. *Sejam R um anel, M um R-módulo e $P \in Max(R)$. Suponhamos que o anel de frações à direita $R_P = R[S_P^{-1}]$ existe. Então um submódulo N de M é S_P-saturado se, e somemete se, existe um submódulo K de M_P tal que $N = h^{-1}(K)$, onde $h : M \longrightarrow M_P$ é a aplicação canônica.*

Demonstração:

Pela Proposição 1.21 existe uma correspondência biunívoca entre submódulos S_P-saturados de M e os submódulos K de $M_P = M[S_P^{-1}]$. Com isso o lema segue trivialmente. □

Para o próximo corolário necessitamos das seguintes definições:

Definição 4.10. *Um anel R é dito localizável à direita se para qualquer ideal maximal à direita P de R existe o anel de frações à direita R_P de R.*

Em ([3], Theorem 1), Brungs mostrou que se R é um domínio ou um anel noetheriano à direita, então R é distributivo se, e somente se, S_P é um conjunto de Ore à direita e R_p é um anel de cadeia à direita, para todo $P \in Max(R)$. Os argumentos de Brungs facilmente se generalizaram para o caso em que R é um anel localizável à direita.

Recentemente, Puninsk ([13]) e Tuganbaev ([18]) construíram exemplos de anéis distributivos à direita que não são localizáveis.

O Corolário 4.8 estende o resultado de Brungs mesmo para anéis não localizáveis, onde S_P é um sistema de Ore, mas não necessariamente reversível à direita.

Pelo que fizemos até aqui, obtemos também uma caracterização dos anéis de Prüfer à direita, que registramos no próximo corolário.

Definição 4.11. *Um anel R é dito anel de Prüfer à direita se R é localizável e para qualquer $P \in Max(R)$ o anel de frações R_P é um anel de cadeia à direita.*

Corolário 4.12. *Um anel R é de Prüfer à direita se, e somente se, R é localizável à direita e, para qualquer $P \in Max(R)$, o reticulado dos ideais à direita S_P-saturados de R é linearmente ordenada por inclusão.*

4.2 Submódulos Saturados

A seção anterior justifica um aprofundamento no estudo dos submódulos saturados, o qual faremos agora. Começamos com uma definição que nos será útil.

Definição 4.13. *Sejam R um anel e M um R-módulo. Um submódulo N de M é dito completamente primo se para $x \notin N$ e $a \in R$ com $xa \in N$ sempre teremos $Ma \subseteq N$.*

O próximo resultado mostra que no caso de ideais bilaterais, tomando o anel R como um R-módulo, os conceitos de submódulos completamente primos e ideais completamente primos coincidem.

Lema 4.14. *Seja R um anel. Se P é um ideal (bilateral) de R então, tomando R como um R-módulo à direita, P é um submódulo completamente primo se, e somente se, P é um ideal completamente primo de R.*

Demonstração:

Suponhamos que P é um ideal completamente primo de R. Sejam $x \notin P$, $a \in R$ com $xa \in P$. Como P é um ideal completamente primo, $a \in P$. Pelo fato de P ser um ideal bilateral, temos $Ra \subseteq P$. Reciprocamente, suponhamos que P é um submódulo completamente primo de R, onde R é visto como um

R-módulo à direita. Sejam $x, y \in R$ tais que $xy \in P$ com $x \notin P$. Por definição de submódulo primo obtemos $Ry \subseteq P$ e isto implica que $y \in P$. Portanto P é um ideal completamente primo. $\square$

Para um submódulo N de M, onde M é um R-módulo à direita, definimos o ideal multiplicativo à direita associado à N

$P_r(N) = \{a \in R : \textit{existe } x \notin N \textit{ com } xa \in N\}$.

Proposição 4.15. *Sejam R um anel, M um R-módulo, N um submódulo de M e P é um ideal completamente primo de R tal que S_P é um conjunto de Ore à direita. Então N é S_P-saturado se, e somente se, $P_r(N) \subseteq P$.*

Demonstração:

Suponhamos que N é S_P-saturado. Então $N = N{S_P}^{-1}$. Tomando $a \in P_r(N)$ segue que existe $x \notin N$ com $xa \in N$. Conseqüentemente $a \in P$ pois caso contrário teríamos $x \in N{S_P}^{-1} = N$, o que é um absurdo. Reciprocamente, assumimos $P_r(N) \subseteq P$ e tomemos $x \in N{S_P}^{-1}$. Então $xs \in N$, para certo $s \in S_P$. Segue que $x \in N$, pois se x não pertencesse a N, s pertenceria a $P_r(N) \cap S_P$, o que é um absurdo. $\square$

A próxima proposição nos dá uma condição suficiente para que o radical de Jacobson de um módulo M seja completamente primo. A recíproca vale quando $M = R_R$.

Proposição 4.16. *Sejam R um anel admissível e M um R-módulo. Se o radical de Jacobson de M é S_P-saturado para todo $P \in Max(R)$, então $J(M)$ é um submódulo completamente primo de M. Em particular, o radical de Jacobson $J(R)$ de R é S_P-saturado para todo $P \in Max(R)$ se, e somente se, $J(R)$ é um ideal completamente primo de R.*

Demonstração:

Suponhamos que $J(M)$ é S_P-saturado, isto é, $(J(M))S_P{}^{-1} = J(M)$. Sejam $x \in M\backslash J(M)$ e $a \in R$ tais que $xa \in J(M)$. Então $a \in P$, pois se $a \in S_P$ teríamos que $x \in J(M)$, pois $J(M)$ é S_P-saturado. Segue que $a \in P$ para todo $P \in Max(R)$, isto é, $a \in J(R)$. Conseqüentemente $Ma \subseteq MJ(R) \subseteq J(M)$, pelo Lema 1.10, e portanto $J(M)$ é completamente primo. Para ver a recíproca desta afirmação quando $M = R_R$, basta observarmos que $J(R)$ é um ideal completamente primo e $xs \in J(R)$, para algum $s \in S_P$, com $x \notin J(R)$, então $s \in J(R) = \bigcap_{P \in Max(R)} P$, o que é uma contradição. $\square$

Para o próximo corolário usaremos a definição de cintura.

Definição 4.17. *Seja R um anel e I um ideal de R. I é dito uma cintura à direita de R se, para qualquer ideal à direita K de R, temos $I \subseteq K$ ou $K \subseteq I$. Definição similar é dada quando I é um submódulo de um R-módulo à direita M.*

Corolário 4.18. *Sejam R um anel admissível, M um R-módulo distributivo e N um submódulo de M. Se $P_r(N) \subseteq J(R)$, então N é uma cintura de M.*

Demonstração:

Suponha que $x \in N$ e $y \notin N$. Vamos mostrar que $N \subseteq yR$. Para tanto tomemos $P \in Max(R)$. Como M é distributivo a Proposição 4.3 nos garante que existe $s \notin P$ tal que $xs \in yR$ ou $ys \in xR \subseteq N$. No segundo caso temos que $s \in P_r(N) \cap S_P$, o que é um absurdo pois $P_r(N) \subseteq J(R)$ e $s \notin J(R)$. Segue que $x \in (yR)S_P{}^{-1}$, para todo $P \in Max(R)$, e pelo Lema 4.4 obtemos $x \in yR$, uma vez que $yR = \bigcap_{P \in Max(R)} (yR)S_P{}^{-1}$. Logo $N \subseteq yR$ e concluímos que N é um cintura. $\square$

Proposição 4.19. *Sejam R um anel admissível e M um R módulo distributivo tal que para todo elemento não nulo $x \in M$ o anulador à direita de x*

está contido em $J(R)$. Para um submódulo N de M as seguintes condições são equivalentes:

(i) N é uma cintura de M.

(ii) N é S_P-saturado, para todo $P \in Max(R)$.

(iii) $P_r(N) \subseteq J(R)$.

Demonstração:

Sabemos que (ii) e (iii) são equivalentes pela Proposição 4.15 e que o Corolário 4.18 nos garante que (iii) implica (i). Vamos mostrar que (i) implica (iii). Para tanto, consideremos que N é uma cintura e, por absurdo, suponhamos que $P_r(N) \nsubseteq J(R)$. Então existe $a \in P_r(N) \backslash J(R)$. Segue que $xa \in N$ para certo $x \notin N$. Como N é uma cintura, $N \subset xR$. Afirmamos que $N = x(N : x)$ e $(N : x) \nsubseteq P$, para algum $P \in Max(R)$. De fato, $N = x(N : x)$ é óbvio uma vez que $(N : x) = \{r \in R \mid xr \in N\}$ e N é uma cintura. Para a outra afirmação basta observar que, se a pertencesse a todos os ideais primos maximais, a pertenceria a $J(R)$, o que é um absurdo. Portanto existe $P \in Max(R)$, tal que $(N : x) \nsubseteq P$. Voltando à demonstração, usaremos novamente o fato de N ser cintura e compararemos N e xP. Se $xP \subseteq N$, temos $P \subset (N : x)$. Então $(N : x) = R$, uma vez que P é maximal. Conseqüentemente $x \in N$, o que é um absurdo. Portanto $N \subset xP$. Tomemos $b \in (N : x)$. Segue que $xb \in N = x(N : x)$ e isto implica que $xb = xp$, para certo $p \in P$, isto é, $x(b - p) = 0$. Portanto $(b - p) \in r(x) \subseteq J(R) \subseteq P$ e temos que $b \in P$. Como $b \in (N : x)$ é qualquer, $(N : x) \subseteq P$, o que também é uma contradição. Logo devemos ter $P_r(N) \subseteq J(R)$. $\square$

O seguinte resultado é conseqüência imediata da proposição 4.19 e 4.16.

Corolário 4.20. *Seja R um anel distributivo à direita tal que o anulador* *à direita de qualquer elemento de R está contido em $J(R)$. Então $J(R)$ é um ideal completamente primo se, e somente se, é uma cintura como ideal à direita.*

Muitos resultados provados em [17] para domínios distributivos à direita podem ser generalizados para anéis distributivos à direita, usando as técnicas desenvolvidas em [7]. Para darmos alguns exemplos, apresentaremos os próximos dois resultados.

Antes de enunciá-los, lembremos que um ideal I de R é dito completamente semiprimo se para todo $a \in R$ tal que $a^2 \in I$ temos que $a \in I$.

Teorema 4.21. *Sejam R um anel distributivo à direita, P um ideal (bilateral) completamente primo de R e $L \subseteq P$ um ideal (bilateral) completamente semiprimo de R que é S_P-saturado como ideal à direita. Então L é um ideal completamente primo.*

Demonstração:

Sejam $a, b \in R$ tais que $ab \in L$. Como L é ideal bilateral de R obtemos $(ba)^2 = (ba)(ba) = b(ab)a \in L$. Pelo fato de L ser completamente semiprimo segue que $ba \in L$. Pela Proposição 4.3 existe $s \notin P$ tal que $as \in bR$ ou $bs \in aR$. Assumimos que $bs = ar$, para certo $r \in R$. Multiplicando a igualdade por b à esquerda temos $bbs = bar = (ba)r$. Como $ba \in L$ obtemos $b^2s = bar \in L$ e portanto $b^2 \in L$ uma vez que L é S_P-saturado como ideal à direita. Usando o fato de L ser um ideal completamente semiprimo concluímos que $b \in L$. Analogamente, $a \in L$, se considerarmos $as \in bR$. Logo L é um ideal completamente primo. $\square$

Corolário 4.22. *Seja R um anel distributivo à direita. As seguintes sentenças são equivalentes:*

(i) $J(R)$ é um ideal completamente primo de R.

(ii) $J(R)$ é S_P-saturado como um ideal à direita, para todo $P \in Max(R)$.

(iii) $J(R)$ é S_P-saturado como um ideal à direita, para algum $P \in Max(R)$.

Demonstração:

Pela Proposição 4.16, (i) e (ii) são equivalentes. Obviamente (ii) implica (iii). Finalmente, se $J(R)$ é S_P-saturado como um ideal à direita para algum $P \in Max(R)$, então o Teorema 4.21 nos garante que $J(R)$ é completamente primo pois como $J(R)$ é a intesecção de ideais completamente primos, $J(R)$ é completamente semiprimo. $\square$

Observemos que, no Exemplo 3.21, obtivemos que $K = J(R)$ é um ideal completamente primo e uma cintura de R.

Tomando $P = \left\{ \begin{bmatrix} p\mathbb{Z} & \mathbb{Q} \\ 0 & p\mathbb{Z} \end{bmatrix} \mid p \in \mathbb{Z}, p\; primo \right\} \in Max(R)$, onde R é o anel de todas as matrizes da forma $\begin{bmatrix} z & q \\ 0 & z \end{bmatrix}$, com $z \in \mathbb{Z}$ e $q \in \mathbb{Q}$ e $K = \left\{ \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix} \in R \,|\, q \in \mathbb{Q} \right\}$. Vamos reobter este resultado usando as demonstrações feitas neste capítulo. Faremos isto mostrando que o S_P-saturamento de K é o próprio K, isto é, $K{S_P}^{-1} = K$. De fato, seja $x \in K{S_P}^{-1}$. Então existe $s \in S_P$ tal que $xs \in K$. Escrevendo $s = \begin{bmatrix} a & q_1 \\ 0 & a \end{bmatrix}$, com $a \notin p\mathbb{Z}$, $q_1 \in \mathbb{Q}$ e $x = \begin{bmatrix} b & q_2 \\ 0 & b \end{bmatrix}$, com $b \in \mathbb{Z}$, $q_2 \in \mathbb{Q}$, temos $xa = \begin{bmatrix} a & q_1 \\ 0 & a \end{bmatrix} . \begin{bmatrix} b & q_2 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & aq_2 + bq_1 \\ 0 & ab \end{bmatrix} = \begin{bmatrix} 0 & q_3 \\ 0 & 0 \end{bmatrix}$, onde $q_3 = aq_2 + bq_1 \in \mathbb{Q}$, pois $xs \in K$. Portanto $b = 0$, uma vez que $\mathbb{Z}$ é um domínio e $a \neq 0$. Logo $x \in K$, isto é, K

é S_P-saturado.

Referências Bibliográficas

[1] Atiyah, M.F., Macdonald, I. G.; *"Introduction to comutative algebra"*, Addison-Wesley Publishing company, 1969.

[2] Bessenrodt, C., Brungs, H.H., Törner, G.; *"Right chain rings, Part 1"*, Schriftenreihe des Fachbereichs Math. 181, Duisburg Univ., 1990.

[3] Brungs, H. H.; *Rings whith a distributive lattice of right ideals*, J. Algebra 40(2) 1 (1976), 392-400.

[4] Cohn, P.M.; *"Universal algebra"*, Harper and Row, 1965.

[5] Endler,O; *"Teoria dos números algébricos"*, Projeto Euclides, IMPA, 1986.

[6] Erdogdu, V.; *Distributive modules*, Canad. Math. Bull. 30 (2) (1987) 248-254.

[7] Ferrero, M., Sant'Ana, A.; *On distributive modules and rings*, Result. Math. 44 (2003) 74-85.

[8] Ferrero, M.; *Ideais Primos em Extensões de Anéis*, Atas da XIII Escola de Álgebra, 1994.

[9] Grätzer, G.; *"Lattice theory, first concepts and distributive lattices"*, W.H. Freeman and Company, 1997.

[10] Lam, T.Y.; *"A first course in noncommutative rings"*, Springer-Verlag, 1990.

[11] Marcus, D. A.; *"Number Fields"*, Springer-Verlag, 1977.

[12] Mazurek, R.; *Distributive rings whith Goldie dimension one*, Comm. Algebra 19 (3) (1991), 931-944.

[13] Puninsk, G.; *Projective modules over the endomorphism ring of a biuniform module*, preprint.

[14] Stenström, B.; *"Rings of Quotients, An Introduction to Methods of Ring Theory"*, Springer-Verlag, 1975.

[15] Stephenson, W.; *Lattice isomorphisms between modules (1) endomorphism rings*, J. London Math. Soc. 1 (2) (1969), 177-183.

[16] Stephenson, W.; *Modules whose lattice of submodules is distributive*, Proc. London Math. Soc. 28 (3) (1974) 291-310.

[17] Törner, G., Zima, J.; *Some remarks on linear estructures in right distributive domains*, Forum Math. 11 (1999), 1-15.

[18] Tuganbaev, A. A.; *Distributive rings, uniserial rings of fractions, and endo-Bezout modules*, J. Math. Sciences 114 (2) (2003), 1185-1203.