Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

ANÉIS E MÓDULOS DISTRIBUTIVOS

por

JOSUÉ HUFF JUNG

Porto Alegre, março de 2005.

Dissertação submetida por Josué Huff Jung* como requisito parcial para obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Dr. Miguel Angel Alberto Ferrero

Professor Co-orientador:

Dr. Alveri Alves Sant'Ana

Banca Examinadora:

Dr. Antonio Paques

Dr. Orlando Stanley Juriaans

Data da Defesa: 21 de março de 2005.

---

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Dedico este trabalho à minha avó, Ivônia Deicke Huff, que sempre me apoiou e acreditou nas minhas escolhas.

Agradecimentos

Agradeço especialmente ao meu orientador, Miguel A. A. Ferrero, excelente profissional, pela oportunidade que tive de realizar este trabalho.

Ao meu co-orientador, Alveri A. Sant'Ana, a quem admiro muito, quero agradecer por toda a ajuda e atenção e pelas boas conversas nos intervalos.

À minha família, em especial ao meu irmão, Cristiano , pelo grande incentivo e cumplicidade e à minha avó, Ivônia , pela imensa dedicação, pela lição de vida e pelos almoços e jantas "so gute. Danke schön, großmama!"

Aos meus colegas da Pós-Graduação, pela amizade e incentivo. Em especial, à Virgínia S. Rodrigues, por me ensinar a utilizar o WinEdt, ao Edson Werle, pelas sessões de estudo e à Lisiane Zoch, Valéria Brum e Rodrigo Vecchia pelo companheirismo e apoio psicológico. Valeu galera !!!

Ao CNPq, pela ajuda financeira nesse período de muito estudo e doação.

E, finalmente, quero agradecer a alguém muito especial, que se renova a cada dia, que busca o aprendizado, a conscientização, alguém que sonha e tenta, a cada instante, enxergar o mundo e a si mesmo de uma maneira diferente.

Resumo

Este trabalho tem por objetivo apresentar resultados sobre módulos e anéis distributivos. Vamos estudar a classe dos módulos distributivos, algumas de suas caracterizações e propriedades mais importantes. Concluiremos o trabalho com dois teoremas centrais. O primeiro deles trata da relação existente entre domínios distributivos e domínios de cadeia. O segundo teorema nos fornece um resultado importante sobre o radical primo de um anel distributivo à direita satisfazendo as condições de cadeia sobre os anuladores principais à direita.

Abstract

The purpose of this work is to present results about distributive rings and modules. We will study the class of distributive modules, some of its characterizations and main proprieties. Then we prove two central theorems on distributive rings. The first one gives the connection between distributive domains and chain domains. The second theorem shows a important result about the prime radical of a right distributive ring satisfying ascending (descending) chain conditions on principal right annihilators.

Índice

Introdução

Um módulo M é dito distributivo se o reticulado de submódulos é distributivo em relação à soma e à intersecção, isto é, $(A+B)\cap C = (A\cap C)+(B\cap C)$ para quaisquer submódulos A, B e C do módulo M. Se considerarmos um anel R como sendo um R-módulo à direita sobre si mesmo, temos que o reticulado de ideais à direita de R é exatamente igual ao reticulado de submódulos do módulo R_R. Dizemos então, que R é distributivo à direita se $(A + B) \cap C = (A \cap C) + (B \cap C)$ para quaisquer ideais à direita A, B e C de R.

Estas estruturas algébricas têm um papel bastante relevante. Muitos trabalhos já foram publicados tendo os anéis e os módulos distributivos como objeto de estudo. Os artigos [2] e [20] estão entre aqueles que marcaram o início de um estudo sistemático de módulos distributivos sobre anéis não-comutativos. Um tratado sobre o assunto com bibliografia completa pode ser encontrado em [21].

O objetivo deste trabalho é apresentar resultados básicos da teoria dos anéis e módulos distributivos e culminará em dois teoremas centrais.

No primeiro capítulo vamos apresentar as noções indispensáveis ao desenvolvimento dos resultados que serão demonstrados posteriormente. Há uma seção dedicada a reticulados e outra a anéis quocientes.

O segundo capítulo é baseado no trabalho de R. Mazurek [15], que coletou algumas caracterizações para Módulos Distributivos em [20], apresentando demonstrações mais acessíveis que nos trabalhos originais. Na última seção deste capítulo mostraremos que o célebre problema de Koethe, que será elu-

cidado no texto, possui resultado positivo na classe dos anéis distributivos à direita.

No terceiro capítulo temos por objetivo provar dois teoremas centrais envolvendo os anéis distributivos à direita. Um deles é de H. H. Brungs e aparece em [2] mas a demonstração apresentada neste trabalho é de R. Mazurek [15], utilizando resultados do segundo capítulo. Ele afirma que um domínio R é distributivo à direita, se e somente se, para cada ideal à direita maximal $\mathcal{M}$ de R, a localização à direita $R_{\mathcal{M}}$ de R em $\mathcal{M}$ existe e é um anel de cadeia à direita. O outro teorema foi provado por M. Ferrero e G. Törner em [5] e afirma que se R é um anel distributivo à direita que possui ao menos um ideal completamente primo contido no radical de Jacobson e satisfaz uma das condições de cadeia sobre os anuladores principais à direita, então o radical primo de R é igual ao ideal singular à direita de R e é completamente primo e nilpotente.

Este último resultado é mais geral do que o proposto por E. C. Posner em [17] cuja demonstração está incompleta. Apesar disso, a afirmação de E. C. Posner é verdadeira e serviu de motivação para uma prova do teorema de M. Ferrero e G. Törner mencionado acima. Então, neste trabalho, o resultado de E. C. Posner é apresentado como um corolário do teorema de M. Ferrero e G. Törner no Capítulo 3.

Capítulo 1

Pré-Requisitos

A finalidade deste capítulo é apresentar definições e resultados que serão utilizados posteriormente. Vamos supor conhecidas as principais noções básicas de Teoria de Anéis e Módulos.

1.1 Conceitos básicos

Consideraremos um anel R sempre associativo e com unidade, mas não necessariamente comutativo. Quando um ideal I de R for bilateral, diremos simplesmente que I é um ideal de R e denotaremos por $I \lhd R$. No caso de I ser ideal à direita a notação é $I <_d R$, e à esquerda, $I <_e R$. Um anel R é chamado simples se seus únicos ideais são os triviais, ou seja, 0 e R.

Quando escrevemos $\subset$ ou $\supset$ estamos considerando inclusão estrita, caso contrário utilizaremos $\subseteq$ ou $\supseteq$.

Um elemento $a \in R$ é dito um divisor de zero à direita se existe um elemento $0 \neq b \in R$ tal que $ab = 0$. Denotaremos por $N_d(R)$ o conjunto de todos os divisores de zero à direita de R. Analogamente, define-se um divisor de zero à esquerda. Dizemos que um elemento $r \in R$ é regular se não é divisor de zero à esquerda nem à direita. Um anel R é um domínio se para quaisquer $a, b \in R$ tivermos $ab = 0$ implica $a = 0$ ou $b = 0$.

Um elemento $a \in R$ é dito invertível à direita (respectivamente à esquerda) se existe $b \in R$ tal que $ab = 1$ (respectivamente $ba = 1$). Um elemento invertível é um elemento que é invertível à esquerda e à direita. O conjunto

de todos os elementos invertíveis do anel R será denotado por $U(R)$. É fácil ver que $U(R)$ é um grupo multiplicativo.

Um elemento t (respectivamente um ideal I) de um anel R é dito nilpotente se existe $n \geq 1$ tal que $t^n = 0$ (respectivamente, $I^n = 0$). O conjunto de todos os elementos nilpotentes de um anel R será denotado por $T(R)$. Um ideal I de R é dito um nil ideal se todo elemento de I é nilpotente.

Definição 1.1. *Um ideal I de um anel R é dito T-nilpotente à direita se para qualquer seqüência $(x_i)_{i\in\mathbb{N}}$ de elementos de I, existe $n \in \mathbb{N}$ tal que $x_n x_{n-1} \dots x_2 x_1 = 0$.*

Definição 1.2. *Um ideal P de um anel R é:*

- *completamente primo, se $P \neq R$ e $\forall\ a, b \in R$ $(ab \in P \Rightarrow a \in P$ ou $b \in P)$*
- *primo, se $P \neq R$ e $\forall\ A, B \lhd R$ $(AB \subseteq P \Rightarrow A \subseteq P$ ou $B \subseteq P)$.*

É fácil verificar que todo ideal completamente primo é primo mas a recíproca não é verdadeira. Como exemplo, basta tomar o anel de matrizes $n \times n$ sobre um corpo K. O ideal nulo é primo mas não é completamente primo. Além disso, um ideal $P \lhd R$ é completamente primo se, e somente se, o anel R/P é um domínio.

O nil radical generalizado $N_g(R)$ de um anel R é igual à intersecção de todos os ideais completamente primos de R e o radical primo $\beta(R)$ é igual à intersecção de todos os ideais primos de R.

O seguinte teorema será utilizado no Capítulo 3 e sua demonstração será omitida com o intuito de não tornar o trabalho muito extenso. Alguns outros resultados deste capítulo também não serão provados, pelo mesmo motivo já citado, ou porque são imediatos ou ainda porque são bem conhecidos. Junto aos resultados mais complexos, é indicada uma bibliografia para o leitor consultá-la havendo interesse.

Teorema 1.3. ([7], Proposição 2.3). *Todo ideal que é T-nilpotente à direita está contido no radical primo $\beta(R)$.*

Definição 1.4. *Um anel R é dito um anel primo se, para quaisquer ideais A e B de R, temos $AB = 0$ implica $A = 0$ ou $B = 0$, isto é, 0 é um ideal primo de R.*

Proposição 1.5. ([13], Capítulo 3, Proposição 4) *Seja P ideal de um anel R tal que $P \neq R$. Então P é um ideal primo se , e somente se, para quaisquer elementos $a, b \in R$, $aRb \subseteq P$ implica $a \in P$ ou $b \in P$.*

Proposição 1.6. *Suponhamos que R seja um anel primo que não é um domínio. Então, $T(R) \neq 0$.*

Demonstração: Pelo fato de R não ser um domínio, existem $a, b \in R$ tais que $a \neq 0$, $b \neq 0$ e $ba = 0$. Como R é um anel primo, o ideal nulo 0 é um ideal primo de R. Logo, por 1.5 temos $aRb \neq 0$. Então, existe $r \in R$ tal que $arb \neq 0$. Mas, $(arb)(arb) = (ar)(ba)(rb) = 0$. Portanto, arb é um elemento não nulo e nilpotente, isto é, $T(R) \neq 0$. □

O radical de Jacobson $J(R)$ de um anel R é definido como a intersecção de todos os ideais à direita maximais de R, isto é,

$J(R) = \bigcap\{\mathcal{M} <_d R : \mathcal{M}$ é ideal à direita maximal de $R\}$.

Em [6], demonstra-se que o radical de Jacobson $J(R)$ é um ideal bilateral de R e que é igual à intersecção de todos os ideais à esquerda maximais de R. Além disso, $x \in J(R)$ se, e somente se, $1 - yxz \in U(R)$ para quaisquer $y, z \in R$.

Proposição 1.7. ([6], Lema. 5.9) *Todo nil ideal à esquerda (direita) de R está contido em $J(R)$.*

Em [6], mostra-se que o radical primo $\beta(R)$ é um nil ideal de R e então, por 1.7 tem-se que $\beta(R) \subseteq J(R)$.

O nil radical $Nil(R)$ de um anel R é, por definição, a soma de todos os nil ideais de R. Novamente em [6], é demonstrado que a soma de qualquer família de nil ideais de R é um nil ideal. Então, o nil radical é o maior nil ideal de R.

Das considerações feitas segue que $\beta(R) \subseteq Nil(R) \subseteq J(R)$.

Denotaremos por $A(R) = \sum\{I <_d R|$ I é nil ideal à direita de R$\}$. Claramente, $\beta(R) \subseteq Nil(R) \subseteq A(R)$. Além disso, da igualdade, $(xy)^{n+1} = x(yx)^n y$, temos que $A(R) = \sum\{L <_e R|$ L é nil ideal à esquerda de R$\}$. Desta forma, $A(R)$ é um ideal de R.

Um anel local R é definido como sendo um anel que possui um único ideal à direita maximal $\mathcal{M}$. Conseqüentemente, $\mathcal{M}= J(R)$. É fácil mostrar que, neste caso, $U(R) = R \setminus J(R)$ e então, $J(R)$ é também o único ideal à esquerda maximal de R.

Se $\mathcal{M}<_d R$ tal que $\mathcal{M} \neq R$ e $R \setminus \mathcal{M} = U(R)$, é imediato que R é um anel local com $J(R) = \mathcal{M}$.

Definição 1.8. *Um anel R é dito um anel de cadeia à direita (respectivamente à esquerda), se para quaisquer ideais à direita (respectivamente à esquerda) A e B de R, temos $A \subseteq B$ ou $B \subseteq A$.*

Claramente, todo anel de cadeia à direita (esquerda) é local.

Proposição 1.9. *Um anel R é de cadeia à direita se, e somente se, para quaisquer $a, b \in R$, $a \in bR$ ou $b \in aR$.*

Dado um subconjunto A de um anel R, o anulador à direita de A em R é, por definição, o ideal à direita de R, $d_R(A) = \{r \in R : Ar = 0\}$. O anulador à esquerda é definido analogamente. Dado $a \in R$, definimos o anulador principal à direita do elemento a em R, como sendo o seguinte ideal à direita de R, $d_R(a) = \{r \in R : ar = 0\}$.

Definição 1.10. *Um anel R é dito fortemente primo à direita se todo ideal não nulo de R contém um subconjunto finito A, cujo anulador à direita em R, $d_R(A)$, é igual a zero.*

Um anel fortemente primo à esquerda é definido analogamente.

Proposição 1.11. *Se R é um anel fortemente primo à direita (esquerda) então R é um anel primo.*

Demonstração: Suponhamos que R é um anel fortemente primo à direita e, por contradição, suponhamos que R não é um anel primo. Então, existem ideais A e B de R tais que $AB = 0$, $A \neq 0$ e $B \neq 0$. Logo, por hipótese, existe $A' = \{a_1, a_2, \ldots, a_n\} \subseteq A$ com $d_R(A') = \{r \in R : A'r = 0\} = \{0\}$. Seja $0 \neq b \in B$. Então, existe $a_i \in A'$ tal que $a_i b \neq 0$. Mas, $a_i b \in AB = 0$, o que é uma contradição. □

Definição 1.12. *Dizemos que um ideal I de um anel R é fortemente primo à direita (respectivamente esquerda), se o anel R/I é fortemente primo à direita (respectivamente esquerda).*

O radical fortemente primo à direita (esquerda) $S_d(R)$, $(S_e(R))$, de um anel R é definido como a intersecção de todos os ideais fortemente primos à direita (esquerda) de R.

Proposição 1.13. *Seja R um anel e $F \subseteq R$ um subconjunto de R. Seja*

$$S = \{x_1 \dots x_n : n \in \mathbb{N},\ x_i \in F \text{ ou } -x_i \in F\}.$$ *Então,*

$$< F >= \{s_1 + \dots + s_m : m \in \mathbb{N}\ ,\ s_i \in S\}$$

é o menor subanel de R que contém F (não necessariamente com unidade) e é chamado de subanel de R gerado por F.

Dizemos que um anel R é Noetheriano à direita se satisfaz a condição de cadeia ascendente (*c.c.a.*) sobre ideais à direita, isto é, se dada uma cadeia qualquer de ideais à direita $I_1 \subseteq I_2 \subseteq \dots$, existe um inteiro positivo k tal que $I_k = I_{k+1} = \dots$ Dizemos que um anel R satisfaz a condição de cadeia ascendente (*c.c.a.*) sobre anuladores principais à direita se, dada uma cadeia qualquer desses ideais à direita $d_R(a_1) \subseteq d_R(a_2) \subseteq \dots$, existe um inteiro positivo k tal que $d_R(a_k) = d_R(a_{k+1}) = \dots$ De forma análoga, poderemos definir a condição de cadeia descendente (*c.c.d.*) sobre anuladores principais à direita, apenas invertendo o sentido das inclusões acima.

Definição 1.14. *Seja $I <_d R$. Dizemos que I é um ideal à direita essencial de R se $I \cap J \neq 0$ para qualquer ideal à direita não nulo J de R.*

Observação 1.15. *É fácil ver que, dado um anel R, se para quaisquer elementos não nulos $a, b \in R$, $aR \cap bR \neq 0$, então qualquer ideal à direita não nulo de R é essencial.*

Proposição 1.16. ([9], Páginas 30 a 36) *Denotemos por*

$$Z(R) = \{\, x \in R : d_R(x) \text{ é um ideal à direita essencial de } R\}.$$

Então $Z(R)$ é um ideal de R que será chamado de ideal singular à direita de R.

Definição 1.17. *Um anel R é dito não singular à direita se $Z(R) = 0$.*

Teorema 1.18. ([10], Teorema 2.2) *Se R é um anel que satisfaz a (c.c.a.) sobre anuladores principais à direita então $R/\beta(R)$ é um anel não singular à direita.*

Proposição 1.19. *Seja R um anel. Se qualquer ideal à direita não nulo de R é essencial então $N_d(R) = Z(R)$ e $Z(R)$ é um ideal completamente primo de R.*

Demonstração: Seja $a \in N_d(R)$. Então existe $0 \neq b \in R$ tal que $ab = 0$, isto é, $d_R(a) \neq 0$. Logo, por hipótese, $d_R(a)$ é essencial. Assim, $a \in Z(R)$. Agora, tome $a \in Z(R)$, ou seja, suponha que $d_R(a)$ é um ideal à direita essencial de R. Então, $d_R(a) \cap R \neq 0$ e assim, existe $0 \neq b \in R$ tal que $b \in d_R(a)$, isto é, $ab = 0$. Logo, $a \in N_d(R)$ e, portanto, $N_d(R) = Z(R) \lhd R$. Para mostrar que $N_d(R)$ é completamente primo, suponhamos $a_1a_2 \in N_d(R)$ com $a_1, a_2 \in R$. Então, existe $0 \neq a \in R$ tal que $a_1a_2a = 0$. Se $a_1 \notin N_d(R)$ temos que $a_2a = 0$ e conseqüentemente $a_2 \in N_d(R)$. □

Como já foi mencionado, vamos supor conhecidas as noções básicas de Teoria de Módulos. Um módulo à direita M sobre o anel R será indicado por M_R e $N < M$ significa que N é um submódulo do módulo M.

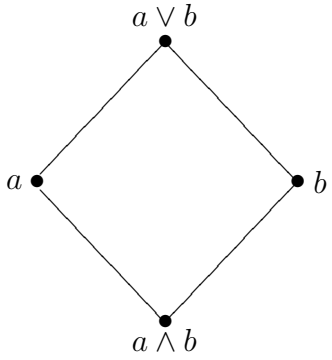
1.2 Reticulados

Definição 1.20. *Um reticulado é um sistema $(S, \leq, \wedge, \vee)$ onde S é um conjunto munido de uma relação de ordem $\leq$ e duas operações binárias $\wedge$, $\vee$ satisfazendo as seguintes condições:*

(i) $c \leq a \wedge b \Leftrightarrow c \leq a$ *e* $c \leq b$, $\forall\ a, b, c \in S$

(ii) $a \vee b \leq c \Leftrightarrow a \leq c$ *e* $b \leq c$, $\forall\ a, b, c \in S$

Em outras palavras, um reticulado é um conjunto ordenado S onde quaisquer dois elementos $a, b \in S$ possuem uma maior cota inferior (ínfimo) $a \wedge b$ e uma menor cota superior (supremo) $a \vee b$, que será representado da seguinte forma:



Na representação acima, subentende-se que a e b não estão relacionados entre si.

Exemplo 1.21. Dado um R-módulo à direita, M_R, seja S o conjunto de todos os submódulos de M_R. É fácil verificar que $(S, \subseteq, \cap, +)$ é um reticulado. No capítulo posterior, diremos simplesmente, que ele é o reticulado de submódulos do módulo M_R. Em particular, se S for o conjunto de todos os ideais à direita de um anel R temos que $(S, \subseteq, \cap, +)$ é um reticulado.

O próximo resultado segue como uma consequência quase imediata da Definição 1.20.

Proposição 1.22. *Seja $(S, \leq, \wedge, \vee)$ um reticulado. Valem as afirmações:*
(i) *A operação $\wedge$ é comutativa, associativa e idempotente.*
(ii) *A operação $\vee$ é comutativa, associativa e idempotente.*
(iii) $a \leq b \Leftrightarrow a \wedge b = a, \ \forall \ a, b, c \in S.$
(iv) $a \leq b \Leftrightarrow a \vee b = b, \ \forall \ a, b, c \in S.$
(v) $a \wedge (a \vee b) = a, \ \forall \ a, b, c \in S.$
(vi) $a \vee (a \wedge b) = a, \ \forall \ a, b, c \in S.$

Proposição 1.23. *Seja $(S, \leq, \wedge, \vee)$ um reticulado e sejam $a, b, x, y \in S$ tais que $x \leq a$ e $y \leq b$. Então, $(x \wedge y) \leq (a \wedge b)$ e $(x \vee y) \leq (a \vee b)$.*

Demonstração: Pelo fato de $\leq$ ser reflexiva, temos que $(x \wedge y) \leq (x \wedge y)$. Então, por 1.20(i), segue que $(x \wedge y) \leq x$ e $(x \wedge y) \leq y$. Pela transitividade de $\leq$ e as hipóteses $x \leq a$ e $y \leq b$ temos que $(x \wedge y) \leq a$ e $(x \wedge y) \leq b$. Novamente, por 1.20(i), conclui-se que $(x \wedge y) \leq (a \wedge b)$. Analogamente, mostra-se que $(x \vee y) \leq (a \vee b)$. □

Definição 1.24. *Um reticulado* $(S, \leq, \wedge, \vee)$ *é dito distributivo se* $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),\ \forall\ a, b, c \in S$.

Proposição 1.25. *Seja* $(S, \leq, \wedge, \vee)$ *um reticulado. Então ele é distributivo se, e somente se,* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),\ \forall\ a, b, c \in S$.

Demonstração: Suponhamos que o reticulado é distributivo. Sejam a, b, c elementos de S. Utilizando, respectivamente, a hipótese, a comutatividade de $\wedge$ e 1.22(v) temos, $(a \vee b) \wedge (a \vee c) = [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] = a \vee [(a \vee b) \wedge c]$. Utilizando novamente os argumentos acima (em outra ordem), 1.22(vi) e a associatividade de $\vee$ podemos concluir que $a \vee [(a \vee b) \wedge c] = a \vee [c \wedge (a \vee b)] = a \vee [(c \wedge a) \vee (c \wedge\ b)] = [a \vee (c \wedge a)] \vee (c \wedge b) = [a \vee (a \wedge c)] \vee (c \wedge b) = a \vee (c \wedge b) = a \vee (b \wedge c)$.
A demonstração no sentido contrário é análoga. □

Proposição 1.26. *Seja* $(S, \leq, \wedge, \vee)$ *um reticulado. Então valem:*
(i) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c),\ \forall\ a, b, c \in S$.
(ii) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c),\ \forall\ a, b, c \in S$.

Demonstração: (i) Sejam a, b, c elementos de S. De 1.20 temos: $(a \wedge b) \leq a$ e $(a \wedge b) \leq b \leq (b \vee c)$. De 1.23 segue que $(a \wedge b) \wedge (a \wedge b) \leq [a \wedge (b \vee c)]$. Mas, $(a \wedge b) \wedge (a \wedge b) = a \wedge b$, pela idempotência de $\wedge$. Logo, podemos concluir que $(a \wedge b) \leq [a \wedge (b \vee c)]$ $(\star)$.

Da mesma forma, temos: $(a \wedge c) \leq a$ e $(a \wedge c) \leq c \leq (b \vee c)$. Segue que, $(a \wedge c) = [(a \wedge c) \wedge (a \wedge c)] \leq [a \wedge (b \vee c)]$ $(\star\star)$. Usando novamente 1.23 em $(\star)$ e $(\star\star)$, concluímos que

$$(a \wedge b) \vee (a \wedge c) \leq [a \wedge (b \vee c)] \vee [a \wedge (b \vee c)] = a \wedge (b \vee c).$$

Portanto, $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

(ii) Sejam $a, b, c \in S$. Temos, $a \leq (a \vee b)$ e $a \leq (a \vee c)$. Logo, podemos concluir que $a = (a \wedge a) \leq (a \vee b) \wedge (a \vee c)$ $(\star)$.

Também, $(b \wedge c) \leq b \leq (a \vee b)$ e $(b \wedge c) \leq c \leq (a \vee c)$. Assim, temos que $b \wedge c = (b \wedge c) \wedge (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ $(\star\star)$. De $(\star)$ e $(\star\star)$, decore

$$a \vee (b \wedge c) \leq [(a \vee b) \wedge (a \vee c)] \vee [(a \vee b) \wedge (a \vee c)] = (a \vee b) \wedge (a \vee c).$$

Portanto, $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$. □

A partir desta proposição, conclui-se que um reticulado $(S, \leq, \wedge, \vee)$ é distributivo se, e somente se, $a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c),\ \forall\ a, b, c \in S$, ou $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge c),\ \forall\ a, b, c \in S$.

Proposição 1.27. *Seja $(S, \leq, \wedge, \vee)$ um reticulado. Se para quaisquer $a, b \in S$ tivermos $a \leq b$ ou $b \leq a$ então o reticulado é distributivo.*

Demonstração: Sejam $a, b, c \in S$. Uma das situações a seguir ocorre:
(i) $a \leq b \leq c$, (ii) $a \leq c \leq b$, (iii) $b \leq a \leq c$, (iv) $b \leq c \leq a$, (v) $c \leq a \leq b$, (vi) $c \leq b \leq a$.
Em qualquer uma das situações teremos,
$a \wedge (b \vee c) = a \wedge c \leq (a \wedge c) \vee (a \wedge b) = (a \wedge b) \vee (a \wedge c)$ ou
$a \wedge (b \vee c) = a \wedge b \leq (a \wedge b) \vee (a \wedge c)$.
Portanto, o reticulado é distributivo. □

Note que a proposição anterior mostra que se S for totalmente ordenado por $\leq$, então o reticulado é necessariamente distributivo.

Definição 1.28. *Um reticulado $(S, \leq, \wedge, \vee)$ é dito modular se satisfaz a seguinte condição: $b \leq c \Rightarrow (a \vee b) \wedge c = (a \wedge c) \vee b,\ \forall\ a, b, c \in S$.*

Proposição 1.29. *Se $(S, \leq, \wedge, \vee)$ é um reticulado distributivo então ele é modular.*

Demonstração: Sejam $a, b, c \in S$ tais que $b \leq c$. Então de 1.22(iii) vem que $b \wedge c = b$. Logo, $(a \wedge c) \vee b = (a \wedge c) \vee (b \wedge c) = (c \wedge a) \vee (c \wedge b) = c \wedge (a \vee b) = (a \vee b) \wedge c$. Portanto, o reticulado é modular. □

Proposição 1.30. *Seja $(S, \leq, \wedge, \vee)$ um reticulado. Então,*
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a),\ \forall\ a, b, c \in S$.

Demonstração: Sejam $a, b, c \in S$. Temos, $(a \wedge b) \leq a \leq (a \vee b)$,
$(a \wedge b) \leq b \leq (b \vee c)$, $(a \wedge b) \leq a \leq (c \vee a)$. Então, por 1.23 temos,
$(a \wedge b) \wedge (a \wedge b) \wedge (a \wedge b) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$, o que implica
$(a \wedge b) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$. Analogamente, $(b \wedge c) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$
e $(c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$. Dessa forma,
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$. □

Proposição 1.31. *Seja* $(S, \leq, \wedge, \vee)$ *um reticulado onde vale:*
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a),\ \forall\ a, b, c \in S.$
Então o reticulado é modular.

Demonstração: Sejam $p, q, r \in S$ tais que $q \leq r$. Vamos mostrar então que $(p \vee q) \wedge r = (p \wedge r) \vee q$.
Temos da hipótese que $(p \wedge q) \vee (q \wedge r) \vee (r \wedge p) = (p \vee q) \wedge (q \vee r) \wedge (r \vee p) (\star)$. Além disso, como $q \leq r$, tem-se: $q \wedge r = q$ e $q \vee r = r$. Logo, conclui-se $(p \wedge q) \vee (q \wedge r) \vee (r \wedge p) = (p \wedge q) \vee q \vee (r \wedge p) = [(p \wedge q) \vee q] \vee (r \wedge p) = q \vee (r \wedge p) = q \vee (p \wedge r) = (p \wedge r) \vee q$. Também, $(p \vee q) \wedge (q \vee r) \wedge (r \vee p) = (p \vee q) \wedge r \wedge (r \vee p) = (p \vee q) \wedge [r \wedge (r \vee p)] = (p \vee q) \wedge r$. Então, de $(\star)$ decorre que $(p \vee q) \wedge r = (p \wedge r) \vee q$. Portanto, o reticulado é modular. □

Proposição 1.32. *Seja* $(S, \leq, \wedge, \vee)$ *um reticulado. Então ele é distributivo se, e somente se,* $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a),\ \forall\ a, b, c \in S.$

Demonstração: Suponhamos que o reticulado seja distributivo. Sejam a, b, c elementos de S. Utilizando a hipótese e a Proposição 1.22 temos:
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = [(a \wedge b) \vee (b \wedge c)] \vee (c \wedge a) =$
$\big\{[(a \wedge b) \vee (b \wedge c)] \vee c\big\} \wedge \big\{[(a \wedge b) \vee (b \wedge c)] \vee a\big\} =$
$\big\{(a \wedge b) \vee [(b \wedge c) \vee c]\big\} \wedge \big\{[a \vee (a \wedge b)] \vee (b \wedge c)\big\} = [(a \wedge b) \vee c] \wedge [a \vee (b \wedge c)] =$
$[c \vee (a \wedge b)] \wedge [a \vee (b \wedge c)] = [(c \vee a) \wedge (c \vee b)] \wedge [(a \vee b) \wedge (a \vee c)] =$
$[(c \vee a) \wedge (b \vee c)] \wedge [(c \vee a) \wedge (a \vee b)] = (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$

Reciprocamente, suponhamos que $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) =$
$(a \vee b) \wedge (b \vee c) \wedge (c \vee a) \forall\ a, b, c \in S$. Sejam $x, y, z \in S$. Então vamos mostrar que $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Temos, $x \wedge (y \vee z) = (x \wedge x) \wedge (y \vee z) =$
$\big\{[x \wedge (x \vee y)] \wedge [x \wedge (x \vee z)]\big\} \wedge (y \vee z) = \big\{[x \wedge (x \vee y) \wedge x] \wedge (x \vee z)\big\} \wedge (y \vee z) =$
$\big\{[x \wedge (x \vee y)] \wedge (x \vee z)\big\} \wedge (y \vee z) = x \wedge [(x \vee y) \wedge (y \vee z) \wedge (z \vee x)] =$
$x \wedge [(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)] = x \wedge \big\{(y \wedge z) \vee [(x \wedge y) \vee (z \wedge x)]\big\} =$
$\big\{(y \wedge z) \vee [(x \wedge y) \vee (z \wedge x)]\big\} \wedge x.$

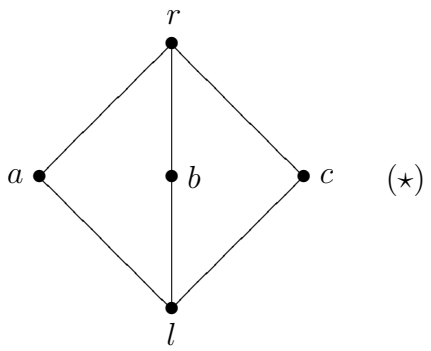
Sabemos que $(x \wedge y) \leq x$ e $(z \wedge x) \leq x$. Então, utilizando a Proposição 1.23, temos que $[(x \wedge y) \vee (z \wedge x)] \leq (x \vee x) = x$. Também sabemos que o

reticulado é modular (pela proposição anterior). Assim, podemos concluir $\big\{(y \wedge z) \vee [(x \wedge y) \vee (z \wedge x)]\big\} \wedge x = [(y \wedge z) \wedge x] \vee [(x \wedge y) \vee (z \wedge x)] =$ $[y \wedge (z \wedge x)] \vee [(z \wedge x) \vee (x \wedge y)] = \big\{[y \wedge (z \wedge x)] \vee (z \wedge x)\big\} \vee (x \wedge y) =$ $\big\{(z \wedge x) \vee [(z \wedge x) \wedge y]\big\} \vee (x \wedge y) = (z \wedge x) \vee (x \wedge y) = (x \wedge y) \vee (z \wedge x) =$ $(x \wedge y) \vee (x \wedge z)$. Portanto, o reticulado é distributivo. □

Definição 1.33. *Seja $(S, \leq, \wedge, \vee)$ um reticulado e S' um subconjunto de S. Dizemos que $(S', \leq, \wedge, \vee)$ é um subreticulado de $(S, \leq, \wedge, \vee)$, se valer a seguinte condição:*

$x, y \in S' \Rightarrow (x \wedge y) \in S'$ *e* $(x \vee y) \in S'$.

Teorema 1.34. *Um reticulado modular $(S, \leq, \wedge, \vee)$ é distributivo se, e somente se, não contém um subreticulado da forma:*



$(\star)$

(*Estamos supondo com a representação* $(\star)$ *que a, b e c são elementos de S que não estão relacionados entre si, $a \vee b = a \vee c = b \vee c = r$ e $a \wedge b = a \wedge c = b \wedge c = l$. Além disso, $a \leq r$, $b \leq r$, $c \leq r$, $l \leq a$, $l \leq b$ e $l \leq c$. Utilizando a Proposição* 1.22 *iii) e iv) é fácil verificar que o subconjunto $S' = \{a, b, c, l, r\}$ satisfazendo as condições acima é um subreticulado de S*).

Demonstração: Suponhamos que reticulado é distributivo e suponhamos por absurdo que ele contém um subreticulado da forma $(\star)$. Por 1.32 temos:

$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a) (\star\star)$

Mas, $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = l \vee l \vee l = l$ e $(a \vee b) \wedge (b \vee c) \wedge (c \vee a) = r \wedge r \wedge r = r$.

Logo, de $(\star\star)$ conclui-se que $l = r$ o que é um absurdo.

Reciprocamente, suponhamos que $(S, \leq, \wedge, \vee)$ é um reticulado modular

que não é distributivo. A partir dessas hipóteses, vamos construir um subreticulado da forma ($\star$) e então fica mostrado o que queríamos.

Como o reticulado não é distributivo, por 1.32 existem $x, y, z \in S$ tais que $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \neq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$. Mas por 1.30, temos que $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \leq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

Sejam $l = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ e $r = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

Pelo visto acima, $l \leq r$ porém, $l \neq r$.

Sejam $a = (r \wedge x) \vee l$, $b = (r \wedge y) \vee l$ e $c = (r \wedge z) \vee l$. Temos:

$r \wedge x = (x \vee y) \wedge (y \vee z) \wedge (z \vee x) \wedge x = (x \vee y) \wedge (y \vee z) \wedge x =$

$x \wedge (x \vee y) \wedge (y \vee z) = x \wedge (y \vee z)$. Da mesma forma,

$r \wedge y = (x \vee y) \wedge (y \vee z) \wedge (z \vee x) \wedge y = y \wedge (z \vee x)$. Então,

$a \vee b = [(r \wedge x) \vee l] \vee [(r \wedge y) \vee l] =$

$\big\{[x \wedge (y \vee z)] \vee l\big\} \vee \big\{[y \wedge (z \vee x)] \vee l\big\} =$

$[x \wedge (y \vee z)] \vee l \vee [y \wedge (z \vee x)] =$

$[x \wedge (y \vee z)] \vee [(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)] \vee [y \wedge (z \vee x)] =$

$[x \wedge (y \vee z)] \vee [(x \wedge y) \vee (z \wedge x)] \vee \big\{(y \wedge z) \vee [y \wedge (z \vee x)]\big\} =$

$\big\{[x \wedge (y \vee z)] \vee (x \wedge y)\big\} \vee (z \wedge x) \vee \big\{[y \wedge (z \vee x)] \vee (y \wedge z)\big\}$.

Mas, $(x \wedge y) \leq y \leq (y \vee z) \Rightarrow (x \wedge y) \leq (y \vee z)$ e

$(y \wedge z) \leq z \leq (z \vee x) \Rightarrow (y \wedge z) \leq (z \vee x)$.

Como o reticulado é modular, temos, $\big\{[x \wedge (y \vee z)] \vee (x \wedge y)\big\} =$

$[x \vee (x \wedge y)] \wedge (y \vee z) = x \wedge (y \vee z)$ e

$\big\{[y \wedge (z \vee x)] \vee (y \wedge z)\big\} = [y \vee (y \wedge z)] \wedge (z \vee x) = y \wedge (z \vee x)$.

Logo, $a \vee b = [x \wedge (y \vee z)] \vee (z \wedge x) \vee [y \wedge (z \vee x)] =$

$\big\{[x \wedge (y \vee z)] \vee (z \wedge x)\big\} \vee [y \wedge (z \vee x)]$.

Porém, $(z \wedge x) \leq z \leq (y \vee z) \Rightarrow (z \wedge x) \leq (y \vee z)$.

Então, $a \vee b = \big\{[x \vee (z \wedge x)] \wedge (y \vee z)\big\} \vee [y \wedge (z \vee x)] = [x \wedge (y \vee z)] \vee [y \wedge (z \vee x)]$.

Sabemos que $r \wedge x = x \wedge (y \vee z)$ e $(r \wedge x) \leq x \leq (z \vee x)$. Logo, $[x \wedge (y \vee z)] \leq (z \vee x)$. Então, $a \vee b = [x \wedge (y \vee z)] \vee [y \wedge (z \vee x)] = \big\{y \vee [x \wedge (y \vee z)]\big\} \wedge (z \vee x)$.

Como $y \leq (y \vee z)$, temos, $\big\{y \vee [x \wedge (y \vee z)]\big\} \wedge (z \vee x) =$
$[(x \vee y) \wedge (y \vee z)] \wedge (z \vee x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x) = r$. Portanto, $a \vee b = r$.

Analogamente, podemos mostrar que $b \vee c = c \vee a = r$. Visto que $l \leq r$ e o reticulado é modular, podemos escrever a, b e c como: $a = r \wedge (x \vee l)$, $b = r \wedge (y \vee l)$ e $c = r \wedge (z \vee l)$. Utilizando os argumentos vistos anteriormente para a, b e c escritos desta forma, obtemos: $a \wedge b = b \wedge c = c \wedge a = l$.

Portanto, a, b, c, l e r formam um subreticulado da forma $(\star)$. □

1.3 Anéis Quocientes

Definição 1.35. *Seja R um anel e S um subconjunto de R. Dizemos que S é um sistema multiplicativo quando as seguintes condições são satisfeitas:*
(i) $1 \in S$
(ii) $0 \notin S$
(iii) $x, y \in S \Rightarrow xy \in S$.

Exemplo 1.36. *Seja R um anel e P um ideal de R. Então, $S = R \setminus P$ é um sistema multiplicativo de R se, e somente se, P é um ideal completamente primo de R.*

Definição 1.37. *Seja R um anel e $S \subseteq R$ um sistema multiplicativo. Um anel R' é dito um anel quociente à direita de R, segundo o sistema multiplicativo S, se existe um homomorfismo $\varphi : R \to R'$ tal que:*
(a) *$\varphi(s)$ é invertível, para todo $s \in S$;*
(b) *Qualquer elemento de R' é da forma $\varphi(a)\varphi(s)^{-1}$, para algum $a \in R$ e algum $s \in S$;*
(c) *$\varphi(a) = 0 \Leftrightarrow as = 0$, para algum $s \in S$.*

Teorema 1.38. *Seja $S \subseteq R$ um sistema multiplicativo de um anel R. Um anel quociente à direita R' de R existe se, e somente se, as duas condições a seguir são satisfeitas:*
(1) *Para quaisquer $s \in S$ e $a \in R$, existem $t \in S$ e $b \in R$ tais que $sb = at$ (Condição de Ore à Direita)*
(2) *Dado $a \in R$, se $sa = 0$, para algum $s \in S$, então $at = 0$ para algum $t \in S$.*

Note que a Condição de Ore à Direita pode ser escrita de forma reduzida por:

$$\forall\ s \in S,\ a \in R \quad sR \cap aS \neq \emptyset.$$

Demonstração: Suponhamos que o anel R' existe. Sejam $s \in S$ e $a \in R$. Como $s \in S$, por (a), existe $\varphi(s)^{-1}$. Por (b), $\varphi(s)^{-1}\varphi(a) = \varphi(a')\varphi(s')^{-1}$ para algum $a' \in R$ e algum $s' \in S$. Então, $\varphi(a)\varphi(s') = \varphi(s)\varphi(a')$, isto é, $\varphi(as') = \varphi(sa')$. Temos, $\varphi(as' - sa') = 0$. Por (c), existe $u \in S$ tal que $(as' - sa')u = 0$, ou seja, $as'u = sa'u$. Chamando, $s'u = t \in S$ e $a'u = b \in R$, tem-se $at = sb$. Portanto, vale a Condição de Ore à Direita.

Agora, sejam $a \in R$ e $s \in S$ tais que $sa = 0$. Por (a), $\varphi(s)$ é invertível, logo, existe $\varphi(s)^{-1}$. Então, $sa = 0$ implica $\varphi(sa) = 0$, isto é, $\varphi(s)\varphi(a) = 0$. Conseqüentemente, $(\varphi(s)^{-1}\varphi(s))\varphi(a) = 0$, ou seja, $\varphi(a) = 0$. Utilizando (c), segue que $at = 0$ para algum $t \in S$. Portanto, a condição (2) é verdadeira.

Reciprocamente, suponhamos que as condições (1) e (2) do enunciado do Teorema 1.38 são satisfeitas. Queremos construir R' e $\varphi : R \to R'$ satisfazendo (a), (b) e (c). Vamos denotar R' por RS^{-1}. Tendo em vista que os elementos de RS^{-1} deverão ser da forma "as^{-1}"($a \in R$, $s \in S$) é natural que iniciemos nossa construção trabalhando com $R \times S$. Vamos definir uma relação $\sim$ em $R \times S$ da seguinte maneira:

$(a, s) \sim (a', s') \Leftrightarrow$ existem $b, b' \in R$ tais que $sb = s'b' \in S$ e $ab = a'b' \in R$.

$\sim$ é uma relação de equivalência. De fato, pois se $(a, s) \in R \times S$, temos que $s.1 = s.1 \in S$ e $a.1 = a.1 \in R$, donde vem que $(a, s) \sim (a, s)$, isto é, $\sim$ é reflexiva. Agora, se (a, s), $(a', s') \in R \times S$ são tais que $(a, s) \sim (a', s')$, então existem $b, b' \in R$ tais que $sb = s'b' \in S$ e $ab = a'b' \in R$, ou equivalentemente, $s'b' = sb \in S$ e $a'b' = ab \in R$, donde vem que $(a', s') \sim (a, s)$, ou seja, $\sim$ é simétrica. Finalmente, se (a, s), (a', s'), $(a'', s'') \in R \times S$ são tais que $(a, s) \sim (a', s')$ e $(a', s') \sim (a'', s'')$, então existem $b, b', c, c' \in R$ tais que $ab = a'b'$, $a'c = a''c'$ e $sb = s'b' \in S$, $s'c = s''c' \in S$. Queremos mostrar que existem $g, g' \in R$ tais que $ag = a''g'$ e $sg = s''g' \in S$. Como $s'b'$, $s'c \in S$, segue por (1), que existem $r \in R$ e $t \in S$ tais que $(s'b')r = (s'c)t \in S$. Então, $s'b'r - s'ct = 0$, ou de forma equivalente, $s'(b'r - ct) = 0$. Logo, por (2) existe $t' \in S$ tal que $(b'r - ct)t' = 0$, isto é, $b'rt' = ctt'$. Agora temos, $sbr = s'b'r = s'ct = s''c't \in S$, ou seja, $(sbr)t' \in S$. Mas, $(sbr)t' = (s''c't)t'$.

Então, $s(brt') = s''(c'tt') \in S$. Também, $a(brt') = a'b'rt' = a'ctt' = a''c'tt' = a''(c'tt')$. Chamando de $g = brt'$ e $g' = c'tt'$, tem-se que $sg = s''g' \in S$ e $ag = a''g'$. Logo, $(a, s) \sim (a'', s'')$ o que mostra que $\sim$ é transitiva.

É fácil mostrar que $(a, s) \sim (ar, sr)$ para qualquer $r \in R$ tal que $sr \in S$. Basta tomar $b = r$ e $b' = 1$ na definição de $\sim$. Esta observação vai nos possibilitar trabalhar com $\sim$ mais eficientemente.

Vamos denotar a classe de equivalência de (a, s) por a/s. O conjunto das classes de equivalência $R \times S/\sim$ será o anel RS^{-1} que procuramos. Para definir a soma em $R \times S/\sim$ observemos que quaisquer duas "frações" a_1/s_1, a_2/s_2 podem ser reduzidas a um denominador comum. Mais formalmente, utilizando (1), temos que existem elementos $r \in R$ e $s \in S$ tais que $s_2r = s_1s \in S$. Assim, $a_1/s_1 = (a_1s)/(s_1s)$ e $a_2/s_2 = (a_2r)/(s_2r)$. Definimos

$$(a_1/s_1) + (a_2/s_2) = (a_1s + a_2r)/t \quad \text{onde} \quad t = s_1s = s_2r \in S.$$

Para multiplicar a_1/s_1 por a_2/s_2 utilizamos novamente (1): $s_1 \in S$ e $a_2 \in R$. Então existem $r \in R$ e $s \in S$ tais que $s_1r = a_2s$. Definimos

$$(a_1/s_1) \cdot (a_2/s_2) = (a_1r)/(s_2s) \quad \text{onde } s_1r = a_2s \quad \text{com} \quad r \in R \text{ e } s \in S.$$

Deixamos ao leitor a tarefa de verificar que as operações $+$ e $\cdot$ estão bem definidas. Depois disto, é fácil ver que RS^{-1} satisfaz todas as propriedades de anel. Vamos mostrar que $0/1$ é o neutro da adição e $1/1$ é a unidade do anel. De fato:

$(a_1/s_1) + (0/1) = (a_1s + 0r)/t$ onde $t = s_1s = 1r \in S$. Logo, $(a_1/s_1) + (0/1) = (a_1s)/t$ onde $t = s_1s = r \in S$. Mas, $(a_1s)/t = (a_1s)/(s_1s) = a_1/s_1$, pela observação feita anteriormente.

Agora, $(a_1/s_1) \cdot (1/1) = (a_1r)/(1s)$ onde $s_1r = 1s$, isto é, $s = s_1r$. Logo, $(a_1r)/(1s) = (a_1r)/s = (a_1r)/(s_1r) = a_1/s_1$. Também, $(1/1) \cdot (a_1/s_1) = (1r)/(s_1s)$ onde $1r = a_1s$, isto é, $r = a_1s$. Então, $(1r)/(s_1s) = r/(s_1s) = (a_1s)/(s_1s) = (a_1/s_1)$.

Queremos agora construir um homomorfismo entre R e RS^{-1}. Seja

$$\varphi : R \to RS^{-1}$$
$$a \mapsto a/1$$

φ é homomorfismo de anéis. De fato, pois se $a_1, a_2 \in R$, então $\varphi(a_1) + \varphi(a_2) = a_1/1 + a_2/1 = (a_1s + a_2r)/t$ onde $t = 1.s = 1.r \in S$. Então $t = s = r \in S$ e $(a_1s + a_2r)/t = (a_1s + a_2s)/s = (a_1 + a_2)s/s = (a_1 + a_2)s/(1.s) = (a_1 + a_2)/1 = \varphi(a_1 + a_2)$.

Para a multiplicação temos, $\varphi(a_1)\varphi(a_2) = (a_1/1) \cdot (a_2/1) = (a_1r)/(1s)$ onde $1r = a_2s$, isto é, $r = a_2s$. Logo, $(a_1r)/(1s) = (a_1a_2s)/(1s) = (a_1a_2)/1 = \varphi(a_1a_2)$. Portanto, φ é homomorfismo de anéis.

Precisamos verificar que valem (a), (b) e (c). Em primeiro lugar, note que, dado $s \in S$ temos, $(1/s) \cdot (s/1) = (1r)/(1s')$ onde $sr = ss'$. Então $sr - ss' = 0$, ou seja, $s(r - s') = 0$. Então por (2), existe $s'' \in S$ tal que $(r - s')s'' = 0$, ou equivalentemente, $rs'' = s's''$. Logo, $(1/s) \cdot (s/1) = (1r)/(1s') = r/s' = (rs'')/(s's'') = (s's'')/(s's'') = [1(s's'')]/[1(s's'')] = 1/1$. Da mesma forma, $(s/1) \cdot (1/s) = (sr)/(ss')$ onde $1.r = 1.s'$, isto é, $r = s'$. Logo, $(s/1) \cdot (1/s) = (sr)/(ss') = (ss')/(ss') = [1(ss')]/[1(ss')] = 1/1$. Segue então que vale (a). De fato, dado $s \in S$, temos que $\varphi(s) = s/1$. Pelo que já foi visto, $s/1$ é invertível e seu inverso é $1/s$.

Para mostrar que vale (b), tomemos x um elemento qualquer de RS^{-1}. Temos que $x = a/s$ onde $a \in R$ e $s \in S$. Além disso, observe que
$(a/1) \cdot (1/s) = (ar)/(ss')$ onde $1.r = 1.s'$, ou seja, $r = s'$. Então,
$(a/1) \cdot (1/s) = (ar)/(ss') = (as')/(ss') = a/s$. Portanto,
$x = a/s = (a/1) \cdot (1/s) = \varphi(a)\varphi(s)^{-1}$.

Para verificar (c), suponha que $a \in R$ é tal que $\varphi(a) = 0$. Logo, $a/1 = 0/1$, isto é, $(a, 1) \sim (0, 1)$. Então existem $c, d \in R$ tais que $ac = 0d$ e $1c = 1d \in S$. Logo, $ac = 0$ e $c = d \in S$. Reciprocamente, seja $a \in R$ tal que $as = 0$ para algum $s \in S$. Temos, $\varphi(a) = a/1 = (as)/(1s) = 0/s = (0s)/(1s) = 0/1$. Portanto, vale (c), o que completa a demonstração do teorema. □

Observação 1.39. *Mostra-se que o anel quociente à direita R' de um anel R (quando existe), é único a menos de isomorfismos.*

Observação 1.40. *Dado um anel R e um sistema multiplicativo S, dizemos que S é um Sistema de Ore à direita quando a condição* (1) *do Teorema* 1.38 *é satisfeita.*

Nos próximos capítulos, trabalharemos efetivamente com o sistema mul-

tiplicativo $S = R \setminus P$, onde P é um ideal completamente primo de R. Se existir o anel quociente à direita de R, segundo o sistema multiplicativo S, vamos chamá-lo de localização à direita de R em P e denotá-lo por R_P.

Observe que, se fizermos a suposição adicional de R ser um domínio, a condição (2) do Teorema 1.38 é satisfeita trivialmente. Então, nesse caso particular, obtemos o seguinte resultado a partir do Teorema 1.38:

Corolário 1.41. *Seja P um ideal completamente primo de um domínio R. Então a localização à direita R_P de R em P existe se, e somente se, $S = R\setminus P$ é um Sistema de Ore à direita.*

Proposição 1.42. *Seja R um domínio e P um ideal completamente primo de R. Se a localização à direita R_P de R em P existe, então R_P é um anel local.*

Demonstração: É fácil verificar que

$$PR_P = \left\{ \frac{a}{b} : a \in P,\ b \notin P \right\}$$

é um ideal à direita de R_P. Além disso, se $\dfrac{x}{y} \in R_P$ e $\dfrac{x}{y} \notin PR_P$ então $x \notin P$ e $y \notin P$. Logo, $\dfrac{x}{y}$ é invertível em R_P. De fato, pois

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xr}{xs} \quad \text{onde} \quad yr = ys \ \text{ com } \ r \in R \ e \ s \notin P.$$

Então, $y(r - s) = 0$. Como R é domínio e $y \neq 0$, pois $y \notin P$, temos que $r - s = 0$, isto é, $r = s$. Logo, $\dfrac{x}{y} \cdot \dfrac{y}{x} = \dfrac{1}{1}$. Portanto, R_P é um anel local com $J(R_P) = PR_P$. □

Se considerarmos R um anel comutativo e S um sistema multiplicativo de R, as condições (1) e (2) do Teorema 1.38 são satisfeitas trivialmente. Logo, o anel quociente de R sempre existe. Note que, em Álgebra Comutativa, é usual definir a relação de equivalência em $R \times S$ da seguinte forma:

$(a, s) \sim (a', s') \Leftrightarrow as'u = a'su$ para algum $u \in S$. $(*)$

E anteriormente definimos:

$(a, s) \sim (a', s') \Leftrightarrow \exists\, b, b' \in R$ tais que $sb = s'b' \in S$ e $ab = a'b' \in R$. $(**)$

Observe que, supondo R comutativo, se $(a,s) \sim (a',s')$ segundo $(*)$ então $(a,s) \sim (a',s')$ segundo $(**)$. Basta tomar $b = s'u$ e $b' = su$. A recíproca dessa afirmação também é verdadeira. Basta tomar $u = sb = s'b' \in S$. Logo, os anéis quocientes (localizações), usualmente construídos em Álgebra Comutativa utilizando $(*)$ são casos particulares dos exibidos aqui.

Capítulo 2

Anéis e Módulos Distributivos

Neste capítulo, apresentaremos as noções e resultados principais sobre os anéis e os módulos distributivos. Trataremos também de radicais clássicos nessa classe de anéis.

2.1 Alguns Resultados e Definições

Definição 2.1. *Seja M_R um R-módulo à direita. M_R é chamado de módulo distributivo se o reticulado de submódulos de M é distributivo, isto é, se*

$$\forall\ A, B, C{<}M, \quad (A + B) \cap C = (A \cap C) + (B \cap C).$$

Observação 2.2. *De acordo com a Proposição* 1.25*, temos que um módulo M é distributivo se, e somente se,*

$$\forall\ A, B, C{<}M, \quad (A \cap B) + C = (A + C) \cap (B + C).$$

Considerando um anel R como sendo um R-módulo à direita sobre si mesmo, temos que o reticulado de ideais à direita de R é exatamente igual ao reticulado de submódulos do módulo R_R. Então, obtemos naturalmente como caso particular de 2.1 a seguinte

Definição 2.3. *Seja R um anel. R é chamado de anel distributivo à direita se o reticulado de ideais à direita de R é distributivo, isto é, se*

$$\forall\ A, B, C{<_d}R, \quad (A + B) \cap C = (A \cap C) + (B \cap C).$$

Um anel R é chamado um anel distributivo à esquerda se o reticulado de ideais à esquerda de R é distributivo.

Exemplo 2.4. O objetivo deste exemplo é mostrar que o anel $\mathbb{Z}$ dos números inteiros é distributivo (à direita e à esquerda). Sejam A, B e C ideais não nulos de $\mathbb{Z}$. (Se algum deles for o ideal nulo, a igualdade da Definição 2.3 verifica-se trivialmente). Como $\mathbb{Z}$ é um anel de ideais principais, existem $a, b, c \in \mathbb{Z} \setminus \{0\}$ tais que $A = a\mathbb{Z}$, $B = b\mathbb{Z}$ e $C = c\mathbb{Z}$. É fácil verificar que

$A + B = a\mathbb{Z} + b\mathbb{Z} = mdc\{a, b\}\mathbb{Z}$ e $A \cap B = a\mathbb{Z} \cap b\mathbb{Z} = mmc\{a, b\}\mathbb{Z}$.

Utilizando a notação: $mdc\{x, y\} := (x, y)$ e $mmc\{x, y\} := [x, y]$ temos,

$A + B = (a, b)\mathbb{Z}$ e $A \cap B = [a, b]\mathbb{Z}$. Então,

$(A + B) \cap C = (a\mathbb{Z} + b\mathbb{Z}) \cap c\mathbb{Z} = (a, b)\mathbb{Z} \cap c\mathbb{Z} = [(a, b), c]\mathbb{Z}$ $(*)$

A seguinte propriedade elementar de números inteiros será utilizada em $(*)$:

$\forall\ a, b, c \in \mathbb{Z} \setminus \{0\}$, $[(a, b), c] = ([a, c], [b, c])$. Logo, obtemos,

$(A + B) \cap C = [(a, b), c]\mathbb{Z} = ([a, c], [b, c])\mathbb{Z} = [a, c]\mathbb{Z} + [b, c]\mathbb{Z} = (a\mathbb{Z} \cap c\mathbb{Z}) + (b\mathbb{Z} \cap c\mathbb{Z}) = (A \cap C) + (B \cap C)$.

Portanto, $\mathbb{Z}$ é um anel distributivo (à direita e à esquerda).

Mais adiante, apresentaremos um exemplo de um anel que também é comutativo (como $\mathbb{Z}$) mas que não é distributivo. Vejamos alguns resultados que serão necessários nesse exemplo.

Lema 2.5. *Seja M_R um R-módulo à direita. Então o reticulado de submódulos de M é modular, isto é, para quaisquer submódulos A, B e C de M com $B \subseteq C$ temos* $(A + B) \cap C = (A \cap C) + B$.

Demonstração: Se $x \in (A + B) \cap C$ então $x = a + b$ para algum $a \in A$ e algum $b \in B$. Logo, $a \in C$ pois $a = x - b$ e $x, b \in C$. Portanto, $x \in (A \cap C) + B$.

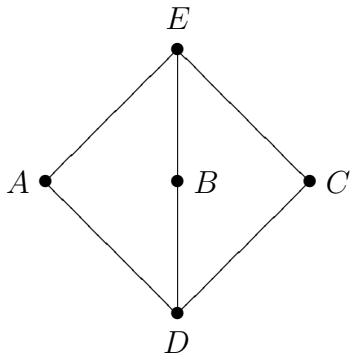
Reciprocamente, se $x \in (A \cap C) + B$ então $x = w + b$ onde $w \in (A \cap C)$ e $b \in B$. Como $B \subseteq C$, temos que $b \in C$ e, conseqüentemente, $x \in C$. Então, $x \in (A + B)$ e $x \in C$. Portanto, $x \in (A + B) \cap C$, o que mostra que o reticulado é modular. □

Utilizando o Lema 2.5 e o Teorema 1.34, obtemos o seguinte

Corolário 2.6. *Para um R-módulo à direita M, as seguintes condições são equivalentes:*

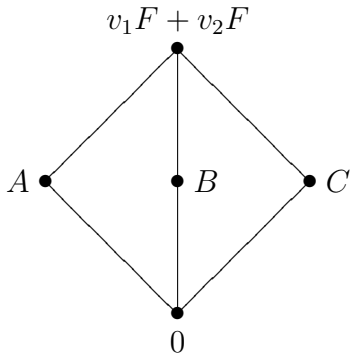
(i) *M_R é distributivo.*

(ii) *O reticulado de submódulos de M_R não contém um subreticulado da forma*



Corolário 2.7. ([15], Lema 1.3) *Seja V um espaço vetorial sobre um corpo F. Se $dim_F V > 1$, então o módulo à direita V_F não é distributivo.*

Demonstração: Visto que $\dim_F V > 1$, existem vetores $v_1, v_2 \in V$ linearmente independentes. Sejam A, B e C os seguintes subespaços vetoriais (submódulos) de V, $A = v_1F$, $B = v_2F$ e $C = (v_1 + v_2)F$. Podemos construir o seguinte subreticulado do reticulado de subespaços de V:



Portanto, pelo corolário anterior, V_F não é distributivo. □

Observação 2.8. *No Corolário* 2.7 *podemos substituir o espaço vetorial por um módulo livre L onde $\{v_1, v_2\}$ são dois elementos da base de L.*

Temos agora ferramentas suficientes para apresentarmos um exemplo de um anel comutativo que não é distributivo.

Exemplo 2.9. Seja $M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}, b \in \mathbb{R} \right\}$.

Este conjunto, juntamente com as operações usuais de soma e multiplicação de matrizes, é um anel comutativo. Para mostrar que M não é distributivo, necessitamos da seguinte observação: Se H é um submódulo de $\mathbb{R}_{\mathbb{Z}}$, isto é, se H é um subgrupo do grupo aditivo $\mathbb{R}$, então o conjunto

$$\begin{pmatrix} 0 & H \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & h \\ 0 & 0 \end{pmatrix} : h \in H \right\} \quad \text{é um ideal de } M.$$

Agora, sejam A, B e C submódulos de $\mathbb{R}_{\mathbb{Z}}$. Então,

$$\left(\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \right) \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & (A+B) \cap C \\ 0 & 0 \end{pmatrix} \quad (1)$$

e

$$\left(\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} \right) + \left(\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} \right) =$$

$$\begin{pmatrix} 0 & (A \cap C) + (B \cap C) \\ 0 & 0 \end{pmatrix} \quad (2)$$

Comparando (1) com (2) percebemos que se $\mathbb{R}_{\mathbb{Z}}$ não é um módulo distributivo então M não é um anel distributivo. Logo, vamos nos concentrar em mostrar que $\mathbb{R}_{\mathbb{Z}}$ não é distributivo. Observe que $\mathbb{R}$ é também um $\mathbb{Q}$-módulo e todo $\mathbb{Q}$-submódulo de $\mathbb{R}$ é também um $\mathbb{Z}$-submódulo de $\mathbb{R}$. Conseqüentemente, se $\mathbb{R}_{\mathbb{Q}}$ não é distributivo então também $\mathbb{R}_{\mathbb{Z}}$ não é distributivo. Note que $\mathbb{R}_{\mathbb{Q}}$ é um espaço vetorial sobre $\mathbb{Q}$ e $\dim_{\mathbb{Q}}\mathbb{R} > 1$. Logo, pelo corolário anterior, tem-se que $\mathbb{R}_{\mathbb{Q}}$ não é distributivo e portanto, M não é distributivo.

Proposição 2.10. *Seja M_R um R-módulo distributivo e N um submódulo de M. Então M/N é um módulo distributivo.*

Demonstração: Sejam A, B e C submódulos de M/N. Então $A = N_1/N$, $B = N_2/N$ e $C = N_3/N$ onde N_1,N_2 e N_3 são submódulos de M tais que $N \subseteq N_i \ \forall\ i \in \{1,2,3\}$. Devemos mostrar que

$$(N_1/N + N_2/N) \cap N_3/N \subseteq (N_1/N \cap N_3/N) + (N_2/N \cap N_3/N).$$

A outra inclusão ocorre, de acordo com a Proposição 1.26.

Seja $x \in (N_1/N + N_2/N) \cap N_3/N$. Então, $x = y + z$, onde $y \in N_1/N$, $z \in N_2/N$ e $x \in N_3/N$. Daí segue que, $y = n_1 + N$ para algum $n_1 \in N_1$,

$z = n_2 + N$ para algum $n_2 \in N_2$ e $x = n_3 + N$ para algum $n_3 \in N_3$. Temos, $x = n_3 + N = (n_1 + N) + (n_2 + N) = (n_1 + n_2) + N$. Conseqüentemente, existem $n, n' \in N$ tais que $n_3 + n = (n_1 + n_2) + n'$ ou, equivalentemente, $n_1 + n_2 = n_3 + (n - n')$. Mas $N \subseteq N_3$, então $(n - n') \in N_3$, donde vem que $(n_1 + n_2) \in N_3$. Como $(n_1 + n_2) \in N_1 + N_2$ e $(n_1 + n_2) \in N_3$ tem-se que $(n_1 + n_2) \in (N_1 + N_2) \cap N_3$.

N_1, N_2 e N_3 são submódulos de M que é distributivo por hipótese, logo, $(N_1+N_2)\cap N_3 = (N_1\cap N_3)+(N_2\cap N_3)$. Então, $(n_1+n_2) \in (N_1\cap N_3)+(N_2\cap N_3)$, isto é, $n_1 + n_2 = h + l$ onde $h \in (N_1 \cap N_3)$ e $l \in (N_2 \cap N_3)$.

Tínhamos que $x = (n_1+n_2)+N$. Logo, $x = (h+l)+N = (h+N)+(l+N)$, onde $h \in (N_1\cap N_3)$ e $l \in (N_2\cap N_3)$. Conseqüentemente, $(h+N) \in N_1/N$ e $(h + N) \in N_3/N$. Também, $(l + N) \in N_2/N$ e $(l + N) \in N_3/N$, isto é, $(h + N) \in (N_1/N \cap N_3/N)$ e $(l + N) \in (N_2/N \cap N_3/N)$. Portanto, $(h + N) + (l + N) = x \in (N_1/N \cap N_3/N) + (N_2/N \cap N_3/N)$. □

Corolário 2.11. *Se R é um anel distributivo à direita e I é um ideal de R então R/I é um anel distributivo à direita.*

Proposição 2.12. *Seja M_R um R-módulo à direita. São equivalentes:*
(i) *M_R é distributivo.*
(ii) $\forall\ a, b, c \in M\ (aR + bR) \cap cR = (aR \cap cR) + (bR \cap cR)$.

Demonstração: Que (i) implica (ii) é imediato. Mostraremos então que (ii) implica (i). Sejam A, B e C submódulos de M. De acordo com 1.26, basta provar que $(A + B) \cap C \subseteq (A \cap C) + (B \cap C)$.

Seja $x \in (A + B) \cap C$. Então, $x = a + b$, onde $a \in A$, $b \in B$ e $x \in C$. Usando a hipótese (ii) tem-se: $(aR+bR)\cap xR = (aR\cap xR)+(bR\cap xR)$. Pelo fato de $x = a + b = a.1 + b.1$ e $x = x.1$, temos que $x \in (aR + bR) \cap xR$ e conseqüentemente $x \in (aR \cap xR) + (bR \cap xR)$. Logo, $x = j + l$ onde $j \in (aR \cap xR)$ e $l \in (bR \cap xR)$. Temos,

$$j = ar_1 = xr_2 \quad \text{para algum} \quad r_1 \in R \quad \text{e algum} \quad r_2 \in R \quad \text{e}$$
$$l = br_3 = xr_4 \quad \text{para algum} \quad r_3 \in R \quad \text{e algum} \quad r_4 \in R.$$

Como $a \in A$ e $x \in C$ temos que $j \in A$ e $j \in C$, isto é, $j \in (A \cap C)$. Analogamente, $l \in (B \cap C)$. Portanto, $j + l = x \in (A \cap C) + (B \cap C)$. □

Exemplo 2.13. $\mathbb{Q}_{\mathbb{Z}}$ é um módulo distributivo. Para verificar essa afirmação, sejam $\frac{a_1}{a_2}, \frac{b_1}{b_2}, \frac{c_1}{c_2} \in \mathbb{Q}$ onde $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}$ e a_2, b_2 e c_2 são não nulos. De acordo com a proposição anterior e com 1.26 basta mostrar que

$$\left(\frac{a_1}{a_2}\mathbb{Z} + \frac{b_1}{b_2}\mathbb{Z}\right) \cap \frac{c_1}{c_2}\mathbb{Z} \subseteq \left(\frac{a_1}{a_2}\mathbb{Z} \cap \frac{c_1}{c_2}\mathbb{Z}\right) + \left(\frac{b_1}{b_2}\mathbb{Z} \cap \frac{c_1}{c_2}\mathbb{Z}\right).$$

A verificação dessa inclusão é bastante simples, bastando efetuar alguns cálculos e utilizar o fato de $\mathbb{Z}$ ser distributivo.

2.2 Algumas Caracterizações de Módulos Distributivos

Nesta seção, serão apresentadas algumas caracterizações importantes para módulos distributivos. Para iniciar, necessitamos do seguinte resultado geral cuja demonstração será omitida porque consiste em cálculos bastante simples e naturais.

Proposição 2.14. *Sejam M_R e N_R módulos à direita sobre o anel R e seja $\alpha : M \to N$ um homomorfismo de módulos. Então,*

a) $\forall\ A < M, \quad \alpha^{-1}\big(\alpha(A)\big) = A + \ker\alpha,$

b) $\forall\ A < N, \quad \alpha\big(\alpha^{-1}(A)\big) = A \cap Im\,\alpha,$

c) $\forall\ A, B < M, \quad \alpha(A+B) = \alpha(A) + \alpha(B),$

d) $\forall\ A, B < N, \quad \alpha^{-1}(A \cap B) = \alpha^{-1}(A) \cap \alpha^{-1}(B).$

O exemplo seguinte mostra que, para submódulos A e B de um módulo M, $\alpha(A \cap B)$ não é necessariamente igual a $\alpha(A) \cap \alpha(B)$.

Exemplo 2.15. ([15], Exemplo 2.1) Seja $M = \left\{x + y\sqrt{2} : x, y \in \mathbb{Z}\right\}$. É fácil verificar que este conjunto, juntamente com as operações usuais de adição de números e multiplicação por elementos de $\mathbb{Z}$, é um $\mathbb{Z}$-módulo.

Seja $\alpha : M \to \mathbb{Z}$, a função dada por $\alpha\left(x + y\sqrt{2}\right) = x$. Então α é um homomorfismo de $\mathbb{Z}$-módulos.

Sejam $A = \mathbb{Z}$ e $B = \left\{x + x\sqrt{2} : x \in \mathbb{Z}\right\}$. É fácil verificar que A e B são submódulos de M e $A \cap B = 0$. Assim, também $\alpha(A \cap B) = 0$.

Por outro lado, $\alpha(A) = \mathbb{Z}$ e $\alpha(B) = \mathbb{Z}$. Logo, $\alpha(A) \cap \alpha(B) = \mathbb{Z}$. Conseqüentemente, $\alpha(A \cap B) \neq \alpha(A) \cap \alpha(B)$.

Como podemos descrever módulos M tais que para qualquer homomorfismo de módulos $\alpha : M \to N$ e quaisquer submódulos A e B de M temos $\alpha(A \cap B) = \alpha(A) \cap \alpha(B)$? Na verdade, o que ocorre é que esta propriedade caracteriza módulos distributivos. De fato, nós temos o seguinte resultado obtido por Stephenson, cuja demonstração apresentada aqui é de Mazurek e encontra-se em ([15], Teorema 2.2):

Teorema 2.16. ([20], Lema 1.4) *Para um R-módulo à direita M as seguintes condições são equivalentes:*

i) *M é distributivo.*

ii) *Para qualquer R-módulo à direita N e qualquer homomorfismo $\alpha : M \to N$, tem-se* $\forall\ A, B < M,\quad \alpha(A \cap B) = \alpha(A) \cap \alpha(B)$.

iii) *Para qualquer R-módulo à direita N e qualquer homomorfismo $\alpha : N \to M$, tem-se* $\forall\ A, B < M,\quad \alpha^{-1}(A + B) = \alpha^{-1}(A) + \alpha^{-1}(B)$.

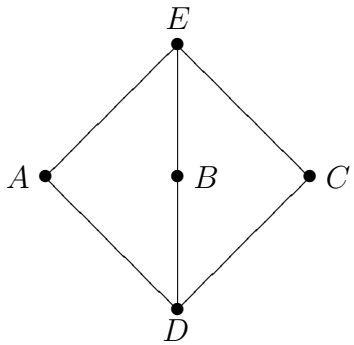
Demonstração: *i)* $\Rightarrow$ *ii)* Suponhamos que M é distributivo e $\alpha : M \to N$ é um homomorfismo de módulos. Sejam A e B submódulos de M. Primeiramente, utilizando a Proposição 2.14, observe que

$$\alpha^{-1}\big(\alpha(A \cap B)\big) \overset{a)}{=} (A \cap B) + \ker\alpha \overset{\text{distrib.}}{=} (A + \ker\alpha) \cap (B + \ker\alpha) \overset{a)}{=} \alpha^{-1}\big(\alpha(A)\big) \cap \alpha^{-1}\big(\alpha(B)\big) \overset{d)}{=} \alpha^{-1}\big(\alpha(A) \cap \alpha(B)\big)\ (*)$$

Conseqüentemente,

$$\alpha(A \cap B) = \alpha(A \cap B) \cap \operatorname{Im}\alpha \overset{b)}{=} \alpha\Big(\alpha^{-1}\big(\alpha(A \cap B)\big)\Big) \overset{(*)}{=} \alpha\Big(\alpha^{-1}\big(\alpha(A) \cap \alpha(B)\big)\Big) \overset{b)}{=} \big(\alpha(A) \cap \alpha(B)\big) \cap \operatorname{Im}\alpha = \alpha(A) \cap \alpha(B).$$

ii) $\Rightarrow$ *i)* Suponhamos que vale (ii) e, por contradição, suponhamos que M não é distributivo. Então, pelo Teorema 2.6, o reticulado de submódulos de M contém um subreticulado da forma



Seja $\alpha : M \to M/C$ o epimorfismo canônico entre os R-módulos M e M/C, isto é, $\alpha(m) = m + C$ para todo $m \in M$. Temos,

$\alpha(A \cap B) = \alpha(D)$. Mas $D \subset C$, então $\alpha(A \cap B) = 0$.
$\alpha(A) = (A + C)/C = E/C$,
$\alpha(B) = (B + C)/C = E/C$.

Assim, $\alpha(A) \cap \alpha(B) = E/C \neq \alpha(A \cap B)$, o que é uma contradição.

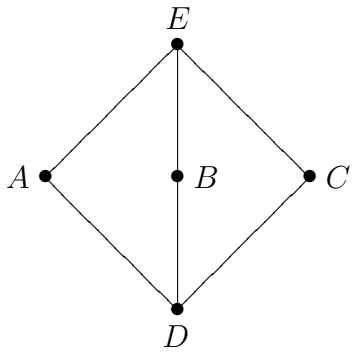
i) $\Rightarrow$ *iii)* Suponhamos que M é distributivo e $\alpha : N \to M$ é um homomorfismo de módulos. Sejam A e B submódulos de M. Utilizando 2.14, temos:

$\alpha\big(\alpha^{-1}(A + B)\big) \overset{b)}{=} (A + B) \cap \operatorname{Im}\alpha \overset{\text{distrib.}}{=} (A \cap \operatorname{Im}\alpha) + (B \cap \operatorname{Im}\alpha) \overset{b)}{=}$
$\alpha\big(\alpha^{-1}(A)\big) + \alpha\big(\alpha^{-1}(B)\big) \overset{c)}{=} \alpha\big(\alpha^{-1}(A) + \alpha^{-1}(B)\big)$ $(**)$

Logo,

$\alpha^{-1}(A + B) = \alpha^{-1}(A + B) + \ker\alpha \overset{a)}{=} \alpha^{-1}\Big(\alpha\big(\alpha^{-1}(A + B)\big)\Big) \overset{(**)}{=}$
$\alpha^{-1}\Big(\alpha\big(\alpha^{-1}(A) + \alpha^{-1}(B)\big)\Big) \overset{a)}{=} \big(\alpha^{-1}(A) + \alpha^{-1}(B)\big) + \ker\alpha = \alpha^{-1}(A) + \alpha^{-1}(B)$.

iii) $\Rightarrow$ *i)* Suponhamos que vale (iii) e, por contradição, suponhamos que M não é distributivo. Então, pelo Teorema 2.6, o reticulado de submódulos de M contém um subreticulado da forma



Seja $\alpha : C \to M$ o homomorfismo inclusão de C em M, isto é, $\alpha(c) = c$ para todo $c \in C$. Então,

$\alpha^{-1}(A + B) = \alpha^{-1}(E) = C$ e
$\alpha^{-1}(A) + \alpha^{-1}(B) = (A \cap C) + (B \cap C) = D + D = D$.

Portanto, $\alpha^{-1}(A + B) \neq \alpha^{-1}(A) + \alpha^{-1}(B)$, o que é uma contradição. $\square$

Proposição 2.17. ([20], Corolário 1,(i)') *Sejam A e B submódulos de um módulo distributivo M_R. Se $A \cap B = 0$ então $Hom_R(A, B) = 0$.*

Demonstração: Seja $f : A \to B$ um homomorfismo qualquer entre os R-módulos A e B, onde estamos supondo $A \cap B = 0$. Devemos mostrar que $f \equiv 0$ ou, equivalentemente, $\ker f = A$. Sejam $N = \{\, a + f(a) : a \in A\}$ e $f(A) = \{\, b \in B : b = f(a)$ para algum $a \in A\}$. N e $f(A)$ são submódulos de M. É imediato que $\big(A + f(A)\big) \cap N = N$.

Além disso, $A \cap N = \ker f$. De fato, tomando $x \in A \cap N$, temos que $x = a + f(a)$ para algum $a \in A$. Então, $x - a = f(a)$. Mas $x - a \in A$, $f(a) \in B$ e $A \cap B = 0$. Logo, $x - a = 0$ e $f(a) = 0$ o que implica $x \in \ker f$. A outra inclusão é óbvia.

Também, $f(A) \cap N = 0$. De fato, se $x \in f(A) \cap N$ então $x = f(a) = a' + f(a')$ para $a, a' \in A$. Logo, $f(a - a') = a'$. Mas, $f(a - a') \in B$, $a' \in A$ e $A \cap B = 0$. Assim, $a' = 0$ e $f(a) = 0$, isto é, $x = 0$.

Pelo fato de M ser distributivo temos que

$$N = \big(A + f(A)\big) \cap N = (A \cap N) + \big(f(A) \cap N\big) = \ker f \subseteq A.$$

Agora, estamos em condições de mostrar que, para qualquer $a \in A$, $f(a) = 0$, isto é, $A = \ker f$. De fato, $a \in A$ implica $a + f(a) \in N \subseteq A$. Logo, $a + f(a) = a'$ para algum $a' \in A$. Então, $a' - a = f(a)$. Mas, $a' - a \in A$, $f(a) \in B$ e $A \cap B = 0$. Conseqüentemente, $f(a) = 0$. □

O teorema a seguir, foi provado também por Stephenson e é uma caracterização de módulos distributivos que será bastante utilizada posteriormente neste trabalho. A demonstração que apresentaremos aqui é de Mazurek e encontra-se em ([15], Teorema 2.3).

Teorema 2.18. ([20], Teorema 1.6 (ii)) *Seja M um módulo à direita sobre um anel R. As duas condições a seguir são equivalentes:*

i) *M é distributivo.*

ii) *Para quaisquer $a, b \in M$ existem $x, y \in R$ tais que $x + y = 1$, $ax \in bR$ e $by \in aR$.*

Demonstração: *i)* $\Rightarrow$ *ii)* Suponhamos que M seja um módulo distributivo. Sejam $a, b \in M$ e denotemos $c = a + b$. Então,

$$c \in (aR + bR) \cap cR = (aR \cap cR) + (bR \cap cR).$$

Assim, $c = cr + cs$ para algum $r \in R$ e algum $s \in R$ com $cr \in aR$ e $cs \in bR$. Para concluir a demonstração, basta tomar $x = s$ e $y = 1 - s$. De fato, $x+y = s+(1-s) = 1$. Além disso, $ax = as = (c-b)s = (cs-bs) \in bR$. Também, $by = b(1-s) = (c-a)(1-s) = c(1-s)-a(1-s) = c-cs-a(1-s) = cr - a(1-s) \in aR$.

$ii) \Rightarrow i)$ Suponhamos que vale (ii). Sejam A, B e C submódulos de M. De acordo com a Proposição 1.26, basta mostrar que

$$(A + B) \cap C \subseteq (A \cap C) + (B \cap C).$$

Seja $c \in (A + B) \cap C$, isto é, $c = (a + b) \in C$ com $a \in A$ e $b \in B$. Por (ii), existem $x, y \in R$ tais que $x + y = 1$, $ax \in bR \subseteq B$ e $by \in aR \subseteq A$. Mas, $cy = (a + b)y = (ay + by) \in aR \subseteq A$. Também, $cy \in cR \subseteq C$. Logo, $cy \in (A \cap C)$. Da mesma forma, $cx = (a+b)x = (ax+bx) \in bR \subseteq B$. Também, $cx \in cR \subseteq C$. Logo, $cx \in (B \cap C)$. Como $c = c \cdot 1 = c(y + x) = cy + cx$, segue que $c \in (A \cap C) + (B \cap C)$. □

Observação 2.19. *A condição ii) do Teorema* 2.18 *pode ser escrita de forma equivalente a:*

ii)' *Para quaisquer* $a, b \in M$, $\{x \in R : ax \in bR\} + \{y \in R : by \in aR\} = R$.

No Capítulo 1, já foi mencionado o fato de que todo anel de cadeia à direita é local. A seguir, daremos um exemplo onde o anel R é local e no entanto não é de cadeia à direita. Logo após, mostraremos uma proposição que nos diz que, se acrescentarmos a hipótese de o anel ser distributivo à direita ao fato de ser local, então ele será de cadeia à direita.

Exemplo 2.20. Seja $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{Q},\ b \in \mathbb{R} \right\}$.

Este conjunto, juntamente com as operações usuais de soma e multiplicação de matrizes, é um anel comutativo. Temos que

$$\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} : r \in \mathbb{R} \right\} \quad \text{é um ideal de } R.$$

Todos os elementos de R que não estão em $\begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}$ são invertíveis. Logo, R é um anel local com $J(R) = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}$. Além disso, R não é distributivo.

De fato: Observe que se H é um submódulo de $\mathbb{R}_{\mathbb{Q}}$, então o conjunto

$$\begin{pmatrix} 0 & H \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & h \\ 0 & 0 \end{pmatrix} : h \in H \right\} \text{ é um ideal de } R.$$

Agora, sejam A, B e C submódulos de $\mathbb{R}_{\mathbb{Q}}$. Então,

$$\left(\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \right) \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & (A+B) \cap C \\ 0 & 0 \end{pmatrix} \quad (1)$$

e

$$\left(\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix} \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} \right) + \left(\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \cap \begin{pmatrix} 0 & C \\ 0 & 0 \end{pmatrix} \right) =$$

$$\begin{pmatrix} 0 & (A \cap C) + (B \cap C) \\ 0 & 0 \end{pmatrix} \quad (2)$$

Comparando (1) com (2) percebemos que se $\mathbb{R}_{\mathbb{Q}}$ não é um módulo distributivo então R não é um anel distributivo. E o fato de $\mathbb{R}_{\mathbb{Q}}$ não ser distributivo já foi justificado no final do Exemplo 2.9. Logo, pela Proposição 1.27, temos que R não é um anel de cadeia (à direita). Portanto, R é um anel local que não é de cadeia.

Proposição 2.21. *Para um anel R as seguintes condições são equivalentes:*

i) *R é um anel de cadeia à direita.*

ii) *R é um anel local e distributivo à direita.*

Demonstração: *i)* $\Rightarrow$ *ii)* É imediato, visto que todo anel de cadeia à direita é local e distributivo à direita de acordo com a Proposição 1.27.

ii) $\Rightarrow$ *i)* Sejam $a, b \in R$. Por 1.9, basta mostrar que $a \in bR$ ou $b \in aR$. Pelo fato de R ser distributivo à direita, utilizando 2.18, existem $x, y \in R$ tais que $x + y = 1$, $ax \in bR$ e $by \in aR$. Claramente, $x \notin J(R)$ ou $y \notin J(R)$.

Desta forma, $x \in U(R)$ ou $y \in U(R)$. Se $x \in U(R)$ então $a \in bR$ e se $y \in U(R)$ então $b \in aR$. □

Vamos aplicar agora esta proposição, no próximo exemplo, para mostrar que a localização do anel dos inteiros $\mathbb{Z}$ em um ideal primo P é um anel de cadeia. Isto foi feito por Mazurek em ([15], Exemplo 2.7).

Exemplo 2.22. Seja $p \in \mathbb{Z}$ um número primo e seja $R = \mathbb{Z}$ o anel dos números inteiros. $P = p\,\mathbb{Z}$ é um ideal primo de R e R é um domínio comutativo. Note que a localização de R em P

$$R_P = \left\{ \frac{r}{s} : \ r, s \in \mathbb{Z}, \ s \notin P \right\}$$

é um anel local comutativo com

$$J(R_P) = \left\{ \frac{r}{s} : \ r, s \in \mathbb{Z}, \ r \in P, s \notin P \right\}$$

Então, pela proposição anterior, para mostrar que R_P é um anel de cadeia, é suficiente mostrar que R_P é um anel distributivo. Para tal, utilizaremos 2.18. Sejam $a, b \in R_P$. Então, $a = \dfrac{a'}{s'}$ e $b = \dfrac{b'}{t'}$. Podemos reduzir a e b a um denominador comum, isto é, escrever $a = \dfrac{a_1}{s}$, $b = \dfrac{b_1}{s}$ com $a_1, b_1, s \in \mathbb{Z}$ e $s \notin P$. Visto que $\mathbb{Z}$ é distributivo, existem $x, y, c, d \in \mathbb{Z}$ tais que $a_1 x = b_1 c$, $b_1 y = a_1 d$ e $x + y = 1$ (por 2.18). Logo,

$$\frac{x}{1}, \frac{y}{1} \in R_P \quad e \quad \frac{x}{1} + \frac{y}{1} = \frac{x+y}{1} = \frac{1}{1}$$

Também,

$$a \cdot \frac{x}{1} = \frac{a_1}{s} \cdot \frac{x}{1} = \frac{a_1 x}{s} = \frac{b_1 c}{s} = \frac{b_1}{s} \cdot \frac{c}{1} = b \cdot \frac{c}{1} \in bR_P$$

$$b \cdot \frac{y}{1} = \frac{b_1}{s} \cdot \frac{y}{1} = \frac{b_1 y}{s} = \frac{a_1 d}{s} = \frac{a_1}{s} \cdot \frac{d}{1} = a \cdot \frac{d}{1} \in aR_P$$

Então, R_P é um anel distributivo e, portanto, é um anel de cadeia.

Observe que os ideais de R_P são $\{P^i R_P : i \geq 0\}$, os quais obviamente formam uma cadeia.

2.3 Radicais Clássicos de Anéis Distributivos à Direita

Esta seção será dedicada a propriedades de alguns radicais clássicos de anéis distributivos à direita. Começaremos mostrando que todo ideal à direita maximal de um anel distributivo à direita é um ideal (bilateral) completamente primo. Precisaremos de dois lemas:

Lema 2.23. *Seja I um ideal de um anel R que é maximal como ideal à direita de R. Então I é um ideal completamente primo de R.*

Demonstração: Sejam $a, b \in R$ tais que $ab \in I$ e $b \notin I$. Temos que $bR+I$ é um ideal à direita de R satisfazendo $b \in bR+I$ e $I \subseteq bR+I$. Mas, $b \notin I$ e I é maximal como ideal à direita de R, então, $bR+I = R$. Logo, existem $r \in R$ e $i \in I$ tais que $br + i = 1$. Temos, $a(br + i) = a.1$ ou, equivalentemente, $(ab)r + ai = a$ o que implica $a \in I$. Portanto, I é um ideal completamente primo de R. □

Lema 2.24. *Se M_R é um módulo distributivo e $\alpha \in End(M_R)$, então:*

i) *Para qualquer submódulo A de M, $\alpha(A) \cap \alpha^{-1}(A) \subseteq A$*

ii) *Para qualquer submódulo A de M, se $\alpha^2(A) \subseteq A+\alpha(A)$ então $\alpha(A) \subseteq A$.*

Demonstração: i) Seja $m \in \alpha(A) \cap \alpha^{-1}(A)$. Então, $m = \alpha(a)$ para algum $a \in A$ e $\alpha(m) \in A$. Pelo fato de M ser distributivo, utilizando o Teorema 2.18, temos que existem $x, y \in R$ tais que $x + y = 1$, $mx \in aR$ e $ay \in mR$. Claramente, $mx \in A$ e $my = \alpha(a)y = \alpha(ay) \in \alpha(mR) = \alpha(m)R \subseteq A$. Desta forma, $m = m.1 = m(x + y) = (mx + my) \in A$.

ii) Suponhamos que $\alpha^2(A) \subseteq A + \alpha(A)$. Então, $\alpha(A) \subseteq \alpha^{-1}\big(A + \alpha(A)\big)$. É fácil ver que $\alpha^{-1}\big(A + \alpha(A)\big) = \alpha^{-1}(A) + \alpha^{-1}\big(\alpha(A)\big)$. Por 2.14 a), temos $\alpha^{-1}(A) + \alpha^{-1}\big(\alpha(A)\big) = \alpha^{-1}(A) + A + \ker\alpha = \alpha^{-1}(A) + A$. Logo, $\alpha(A) \subseteq \alpha^{-1}(A) + A$. Conseqüentemente, $\alpha(A) = \alpha(A) \cap \big(\alpha^{-1}(A) + A\big) = \big(\alpha(A) \cap \alpha^{-1}(A)\big) + \big(\alpha(A) \cap A\big)$. Aplicando agora i), obtemos $\alpha(A) \subseteq A$. □

Corolário 2.25. *Se R é um anel distributivo à direita e A é um ideal à direita maximal de R, então A é um ideal (bilateral) completamente primo de R.*

Demonstração: Para mostrar que A é um ideal de R é suficiente provar que A é um ideal à esquerda de R. Por contradição, suponha que existe $r \in R$ tal que $rA \nsubseteq A$. Como $A + rA$ é um ideal à direita de R, pela maximilidade de A, segue que $A + rA = R$. Seja $\alpha : R \to R$, dado por $\alpha(x) = rx$. Então $\alpha \in End(R_R)$ e $\alpha^2(A) = r^2A \subseteq R = A + rA = A + \alpha(A)$. Conseqüentemente, pelo Lema 2.24,(ii), $\alpha(A) \subseteq A$. Assim, $rA \subseteq A$, o que é uma contradição. Desta forma, A é um ideal de R. Utilizando o Lema 2.23, segue que A é um ideal completamente primo de R. □

Teorema 2.26. ([15], Teorema 4.1) *Seja M_R um módulo distributivo e seja $\alpha \in End(M_R)$. Se A é um submódulo de M tal que para algum $n \in \mathbb{N}$,*

$\alpha^n(A) \subseteq A + \alpha(A) + \alpha^2(A) + \ldots + \alpha^{n-1}(A)$, *então* $\alpha(A) \subseteq A$.

Demonstração: Vamos fazer indução em n. O caso $n = 1$ é óbvio e o caso $n = 2$ foi mostrado no Lema 2.24,(ii). Suponhamos que o resultado é verdadeiro para um certo n e que $\alpha^{n+1}(A) \subseteq A + \alpha(A) + \alpha^2(A) + \ldots + \alpha^n(A)$.

Observe que $A + \alpha(A) + \alpha^2(A) + \ldots + \alpha^n(A) =$

$A + \alpha(A) + \alpha(A) + \alpha^2(A) + \alpha^2(A) + \ldots + \alpha^{n-1}(A) + \alpha^{n-1}(A) + \alpha^n(A) =$

$\big(A + \alpha(A)\big) + \alpha\big(A + \alpha(A)\big) + \alpha^2\big(A + \alpha(A)\big) + \ldots + \alpha^{n-1}\big(A + \alpha(A)\big)$.

Logo,

$\alpha^{n+1}(A) \subseteq \big(A + \alpha(A)\big) + \alpha\big(A + \alpha(A)\big) + \alpha^2\big(A + \alpha(A)\big) + \ldots + \alpha^{n-1}\big(A + \alpha(A)\big)$.

Como, $\alpha^n\big(A + \alpha(A)\big) = \alpha^n(A) + \alpha^{n+1}(A)$ e

$\alpha^n(A) \subseteq \big(A + \alpha(A)\big) + \alpha\big(A + \alpha(A)\big) + \alpha^2\big(A + \alpha(A)\big) + \ldots + \alpha^{n-1}\big(A + \alpha(A)\big)$,

resulta,

$\alpha^n\big(A + \alpha(A)\big) \subseteq \big(A + \alpha(A)\big) + \alpha\big(A + \alpha(A)\big) + \alpha^2\big(A + \alpha(A)\big) + \ldots +$
$\alpha^{n-1}\big(A + \alpha(A)\big)$.

Utilizando a hipótese de indução, temos que $\alpha\big(A + \alpha(A)\big) \subseteq A + \alpha(A)$.

Mas, $\alpha^2(A) \subseteq \alpha(A) + \alpha^2(A) = \alpha\big(A + \alpha(A)\big)$.

Logo, $\alpha^2(A) \subseteq A + \alpha(A)$. Então, pelo Lema 2.24,(ii) segue que $\alpha(A) \subseteq A$. □

O exemplo seguinte mostra que o conjunto $T(R)$ dos elementos nilpotentes de um anel R não é, necessariamente, fechado para a adição e multiplicação.

Após o exemplo, mostraremos que, se R for distributivo à direita, essa última afirmação ocorre. Assim, neste caso, $T(R)$ é um subanel de R (sem unidade).

Exemplo 2.27. ([15], Exemplo 4.2) Seja K um anel e $R = M_2(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K \right\}$.

Observe que

$$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{e}$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Então,

$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in T(R)$. Entretanto,

$$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \notin T(R) \text{ porque}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Também,

$$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \notin T(R) \quad \text{porque}$$

$$\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}.$$

Proposição 2.28. ([15], Proposição 4.3) *Seja R um anel distributivo à direita. Então $T(R)$ é um subanel (sem unidade) de $J(R)$ e $T(R)$ é a soma dos ideais nilpotentes de $T(R)$.*

Demonstração: Seja $t \in T(R)$. Então $t^n = 0$ para algum $n \geq 1$. Seja

$\alpha : R \to R$ definida por $\alpha(r) = tr$. Observe que, encarando R como um módulo à direita sobre si mesmo, α é um homomorfismo de módulos.

Seja $a \in R$ e considere o submódulo $A = aR$ de R_R. Temos,

$$\alpha^n(A) = \alpha^n(aR) = t^n aR = 0$$

Logo, $\alpha^n(aR) = 0 \subseteq aR + \alpha(aR) + \alpha^2(aR) + \ldots + \alpha^{n-1}(aR)$. Então, pelo Teorema 2.26 segue que $\alpha(aR) \subseteq aR$, isto é, $taR \subseteq aR$. Dessa forma, $ta \in aR$. Em resumo, temos:

$$\text{Se } \; t \in T(R) \; \text{ e } \; a \in R \text{ então } \; ta \in aR \; \; (*)$$

De $(*)$, é fácil verificar que

$$t_1, t_2, \ldots, t_n \in T(R), \; a_1, a_2, \ldots, a_n \in R \Rightarrow t_1 a_1 t_2 a_2 \ldots t_n a_n \in a_1 a_2 \ldots a_n R \; (**)$$

Sejam $t_1, t_2 \in T(R)$. Então, $t_1^n = t_2^m = 0$ para algum $n \geq 1$ e algum $m \geq 1$. Supondo $n \geq m$, temos que $t_1^n = t_2^n = 0$. Logo, utilizando $(**)$ segue que $(t_1 t_2)^n \in t_2^n R = 0$ e, desta forma, $t_1 t_2 \in T(R)$.

Além disso, $(t_1 + t_2)^{2n}$ é uma soma de produtos de elementos nilpotentes e em cada um desses produtos t_1 ou t_2 aparece ao menos n vezes. Conseqüentemente, por $(**)$, $(t_1 + t_2)^{2n} = 0$ e, assim, $t_1 + t_2 \in T(R)$. Logo, $T(R)$ é um subanel de R.

Seja $t \in T(R)$ com $t^n = 0$ e seja I o ideal de $T(R)$ gerado por t, isto é, $I = t\mathbb{Z} + tT(R) + T(R)t + T(R)tT(R)$. Observe que todo elemento de I^n é uma soma de produtos de elementos nilpotentes e em cada um desses produtos t aparece ao menos n vezes. Logo, por $(**)$, obtemos que $I^n \subseteq t^n R = 0$. Então, I é um ideal nilpotente de $T(R)$ com $t \in I$. Portanto, o anel $T(R)$ é a soma de seus ideais nilpotentes.

Pelo Corolário 2.25, um ideal à direita maximal de R é um ideal completamente primo de R. E é fácil ver que qualquer elemento nilpotente de R, isto é, qualquer elemento de $T(R)$ está na intersecção de todos os ideais completamente primos de R. Segue então que $T(R) \subseteq J(R)$, ou seja, $T(R)$ é um subanel de $J(R)$. □

Lema 2.29. (*Andrunakievich*) *Se R é um anel, A é um ideal de R, I é um ideal de A (isto é, $I \lhd A \lhd R$) e I^* é o ideal de R gerado por I então $(I^*)^3 \subseteq I$.*

Demonstração: Pelo fato de R ser um anel com unidade, temos que o

ideal I^* de R gerado por I é $I^* = RIR$. Logo, $(I^*)^3 = (RIR)^3 = (RIR)(RIR)(RIR)$. Entretanto, $I \subseteq A \lhd R$. Então, $(RIR)(RIR)(RIR) \subseteq A(RIR)A \subseteq (AR)I(RA) \subseteq AIA$. Agora, utilizando o fato de $I \lhd A$ segue que $AIA \subseteq I$ e portanto, $(I^*)^3 \subseteq I$. □

Existe uma célebre conjectura que denominamos atualmente de problema de Koethe que foi introduzida por G. Koethe em 1930 e não foi resolvida até hoje. Recentemente, na tentativa de resolvê-la, muitos progressos foram feitos, porém uma resposta definitiva e completa não foi dada.

O problema pode ser formulado de várias maneiras elementares equivalentes. Vamos considerar a forma encontrada em ([6], página 87). Sabemos que se I e J são nil ideais bilaterais de R, então $I + J$ é um nil ideal de R. Também, se I e J são ideais à direita (esquerda) nilpotentes de R, então $I + J$ é também nilpotente. Porém, ainda não sabemos responder a seguinte questão:

Problema de Koethe: *A soma de dois nil ideais à direita é também nil ?*

O seguinte teorema mostra, em particular, que $A(R) = \beta(R)$ se R é um anel distributivo à direita. Assim, podemos concluir que o problema de Koethe possui uma solução positiva na classe dos anéis distributivos à direita. De fato, se I e J são dois nil ideais à direita então $I + J \subseteq A(R) = \beta(R)$. Mas, $\beta(R)$ é um nil ideal de R pelo que foi visto no Capítulo 1. Portanto, $I + J$ é um nil ideal à direita de R.

Teorema 2.30. ([15], Teorema 4.4) *Seja R um anel distributivo à direita. Então, $\beta(R) = Nil(R) = A(R)$.*

Demonstração: Em geral, $\beta(R) \subseteq Nil(R) \subseteq A(R)$, conforme visto no Capítulo 1. Então, no caso de R ser distributivo à direita, se mostrarmos que $A(R) \subseteq \beta(R)$, o teorema fica provado. Seja $a \in A(R)$. Então, $a = a_1 + a_2 + \ldots + a_n$ onde $a_i \in T(R)$. Pela Proposição 2.28, T(R) é fechado para a soma e, assim, $a \in T(R)$. Seja I o ideal de $T(R)$ gerado por a, isto é, $I = a\mathbb{Z} + aT(R) + T(R)a + T(R)aT(R)$. Então, pela demonstração da Proposição 2.28, o ideal I é nilpotente e $I \lhd A(R) \lhd R$. Seja I^* o ideal de R gerado por I. Então, pelo lema de Andrunakievich, temos $(I^*)^3 \subseteq I$.

Desta forma, I^* é um ideal nilpotente de R e conseqüentemente, $I^* \subseteq \beta(R)$. Portanto, $a \in \beta(R)$, isto é, $A(R) \subseteq \beta(R)$. □

Lema 2.31. ([15], Lema 4.5) *Seja R um anel distributivo à direita e $U(R)$ o grupo de invertíveis de R. Denotemos por*

$$\rho(R) := \{u_1t_1 + \ldots + u_nt_n : n \in \mathbb{N},\ u_i \in U(R),\ t_i \in T(R)\} \quad e$$

$$\lambda(R) := \{t_1u_1 + \ldots + t_mu_m : m \in \mathbb{N},\ t_i \in T(R),\ u_i \in U(R)\}.$$

Então, $\rho(R) = \lambda(R)$ é um ideal de $J(R)$.

Demonstração: Se $u \in U(R)$ e $t \in T(R)$ então $ut = utu^{-1}u$ e além disso, $utu^{-1} \in T(R)$. Logo, $\rho(R) \subseteq \lambda(R)$. Analogamente, $\lambda(R) \subseteq \rho(R)$. Pela Proposição 2.28, temos que $T(R) \subseteq J(R)$. Logo, $\rho(R) \subseteq J(R)$. De fato, se $x \in \rho(R)$ então $x = u_1t_1 + \ldots + u_nt_n$ onde $t_i \in T(R) \subseteq J(R) \lhd R$, o que implica $x \in J(R)$. Falta mostrar que $\rho(R) \lhd J(R)$. Sabemos que para cada $j \in J(R)$, $1 + j \in U(R)$. Conseqüentemente, se $u \in U(R)$ e $t \in T(R)$ então $jut = (1+j)ut - ut \in \rho(R)$ e $tuj = tu(1+j) - tu \in \lambda(R) = \rho(R)$. Portanto, $\rho(R)$ é um ideal de $J(R)$. □

Teorema 2.32. ([15], Teorema 4.6) *Para um anel distributivo à direita R as seguintes condições são equivalentes:*

a) *R é um domínio.*

b) *R é um anel fortemente primo à direita.*

c) *R é um anel fortemente primo à esquerda.*

Demonstração: *a)* $\Rightarrow$ *b)* Seja I um ideal não nulo de R e $0 \neq i \in I$. Considere $A = \{i\}$. Se $x \in R$ é tal que $x \in d_R(A)$, então $ix = 0$. Como R é um domínio, segue que $x = 0$, isto é, $d_R(A) = 0$. Portanto, R é um anel fortemente primo à direita.

b) $\Rightarrow$ *a)* Suponhamos que R é um anel fortemente primo à direita e, por contradição, suponhamos que R não é um domínio. Por 1.11, R é um anel primo e, então, utilizando 1.6, segue que $T(R) \neq 0$. Logo, $\rho(R)$ definido no lema anterior é não nulo. Seja I o ideal de R gerado por $\rho(R)$. O fato de R ser primo, o lema anterior e o Lema de Andrunakievich implicam $0 \neq I^3 \subseteq \rho(R)$. Conseqüentemente, I^3 contém um subconjunto finito $F = \{a_1, a_2, \ldots, a_n\}$ tal que $d_R(F) = 0$. Visto que $F \subseteq \rho(R)$, todo elemento a_i tem a forma

$a_i = \sum u_{ik}t_{ik}$, onde $u_{ik} \in U(R)$ e $t_{ik} \in T(R)$. Da Proposição 2.28, segue que o subanel S de R gerado por todos os elementos t_{ik} é nilpotente. Se m é um inteiro positivo tal que $S^m \neq 0$ e $S^{m+1} = 0$, então, obtemos $0 \neq S^m \subseteq d_R(F)$, o que é uma contradição.

A equivalência entre (a) e (c) é demonstrada de forma análoga. □

Diretamente do Teorema 2.32, obtemos o seguinte resultado:

Corolário 2.33. *Se R é um anel distributivo à direita então*

$$N_g(R) = S_d(R) = S_e(R).$$

Capítulo 3

Dois Teoremas Centrais

Neste capítulo, iremos provar dois teoremas importantes sobre os anéis distributivos à direita. A demonstração do primeiro deles foi dada por H. H. Brungs ([2], Teorema 1) em 1975 mas a prova que apresentaremos aqui é de R. Mazurek ([15], Teorema 3.7). O outro teorema foi demonstrado por M. Ferrero e G. Törner ([5], Teorema 8). Iniciaremos com uma proposição que trata de localizações em domínios distributivos à direita.

Proposição 3.1. ([15], Proposição 3.4) *Seja P um ideal completamente primo de um domínio distributivo à direita R. Então a localização à direita R_P de R em P existe e R_P é um anel de cadeia à direita.*

Demonstração: Primeiramente, vamos mostrar que R_P existe. Pelo Teorema 1.41, basta provar que a Condição de Ore à direita é satisfeita. De fato, sejam $a \in R$ e $s \in S = R \setminus P$. Visto que R é distributivo à direita, pelo Teorema 2.18, existem $x, y \in R$ tais que $x + y = 1$, $ax \in sR$ e $sy \in aR$. Se $x \in S$, então $ax \in sR \cap aS$, isto é, a Condição de Ore vale. Suponha, que $x \notin S$, ou equivalentemente, $x \in P$. Então, $y \notin P$, e desta forma, também $sy \notin P$. Mas, $sy \in aR$. Logo, $sy = at$ para algum $t \in R$. Visto que $sy \notin P$, segue que $at \notin P$ o que implica $t \notin P$, isto é, $t \in S$. Então, $sy \in sR \cap aS$. Portanto, vale a Condição de Ore, ou seja, R_P existe. De acordo com a Proposição 1.42, R_P é um anel local. Então por 2.21 basta mostrar que R_P é um anel distributivo à direita. Para isso, usaremos 2.18:

Sejam $a, b \in R_P$. Então, existem $a_1, b_1 \in R$ e $s \in S = R \setminus P$ tais que

$a = \dfrac{a_1}{s}$ e $b = \dfrac{b_1}{s}$. Como R é distributivo à direita por hipótese, segue de 2.18, que existem $x, y, z, t \in R$ tais que $x + y = 1$, $a_1 x = b_1 z$ e $b_1 y = a_1 t$.

Claramente, $\dfrac{1}{1} = \dfrac{s}{1} \cdot \dfrac{x+y}{1} \cdot \dfrac{1}{s} = \dfrac{s}{1} \cdot \left(\dfrac{x}{1} + \dfrac{y}{1}\right) \cdot \dfrac{1}{s} = x_1 + y_1$, onde

$x_1 = \dfrac{s}{1} \cdot \dfrac{x}{1} \cdot \dfrac{1}{s}$ e $y_1 = \dfrac{s}{1} \cdot \dfrac{y}{1} \cdot \dfrac{1}{s}$. Além disso, $ax_1 = \dfrac{a_1}{s} \cdot \dfrac{s}{1} \cdot \dfrac{x}{1} \cdot \dfrac{1}{s} = \dfrac{a_1}{1} \cdot \dfrac{x}{1} \cdot \dfrac{1}{s} =$

$\dfrac{a_1 x}{1} \cdot \dfrac{1}{s} = \dfrac{b_1 z}{1} \cdot \dfrac{1}{s} = \dfrac{b_1}{1} \cdot \dfrac{z}{1} \cdot \dfrac{1}{s} = \dfrac{b_1}{s} \cdot \dfrac{s}{1} \cdot \dfrac{z}{1} \cdot \dfrac{1}{s} = b \cdot \dfrac{s}{1} \cdot \dfrac{z}{1} \cdot \dfrac{1}{s} \in bR_P$. Analogamente,

$by_1 \in aR_P$.

Acabamos de mostrar que, dados $a, b \in R_P$, existem $x_1, y_1 \in R_P$ tais que $x_1 + y_1 = 1$, $ax_1 \in bR_P$ e $by_1 \in aR_P$. Logo, R_P é distributivo à direita. Portanto, por 2.21, R_P é um anel de cadeia à direita. □

Teorema 3.2. ([2], Teorema 1) *Para um domínio R as seguintes condições são equivalentes:*

a) *R é um anel distributivo à direita.*

b) *Para cada ideal à direita maximal $\mathcal{M}$ de R, a localização à direita $R_{\mathcal{M}}$ de R em $\mathcal{M}$ existe e $R_{\mathcal{M}}$ é um anel de cadeia à direita.*

Demonstração: *a)* $\Rightarrow$ *b)* Seja $\mathcal{M}$ um ideal à direita maximal de R. Então, pelo Corolário 2.25, $\mathcal{M}$ é um ideal (bilateral) completamente primo de R. Logo, pela Proposição 3.1, a localização à direita $R_{\mathcal{M}}$ existe e $R_{\mathcal{M}}$ é um anel de cadeia à direita.

b) $\Rightarrow$ *a)* Sejam $a, b \in R$, $A = \{x \in R : ax \in bR\}$ e $B = \{y \in R : by \in aR\}$. Então, A e B são ideais à direita de R. Mostraremos que $A + B = R$. Suponha que $A + B \neq R$. Então, $A + B \subseteq \mathcal{M}$ para algum ideal à direita maximal $\mathcal{M}$ de R. Por b), $R_{\mathcal{M}}$ é um anel de cadeia à direita. Assim, por 1.9, $\dfrac{a}{1} \in \dfrac{b}{1} R_{\mathcal{M}}$ ou $\dfrac{b}{1} \in \dfrac{a}{1} R_{\mathcal{M}}$. Suponhamos que $\dfrac{a}{1} \in \dfrac{b}{1} R_{\mathcal{M}}$. Então $\dfrac{a}{1} = \dfrac{b}{1} \cdot \dfrac{r}{s}$ para algum $r \in R$ e algum $s \notin \mathcal{M}$. Utilizando a definição de multiplicação em $R_{\mathcal{M}}$ vista no Capítulo 1, chegamos em $\dfrac{a}{1} = \dfrac{br}{s}$, ou equivalentemente, $(a, 1) \sim (br, s)$. Então, existem $b', b'' \in R$ tais que $1.b' = sb'' \notin \mathcal{M}$ e $ab' = (br)b'' \in R$. Logo, $a.(sb'') = (br)b''$ ou $(as)b'' = (br)b''$. Pelo fato de R ser um domínio, temos $as = br \in bR$, isto é, $s \in A \subseteq \mathcal{M}$ o que é uma contradição.

Conseqüentemente, $\frac{a}{1} \notin bR_{\mathcal{M}}$ e de maneira similar, mostra-se que $\frac{b}{1} \notin \frac{a}{1}R_{\mathcal{M}}$. Desta forma, $A + B = R$ e assim, pela Observação 2.19, segue que o anel R é distributivo à direita. □

Brungs provou também que este teorema é válido substituindo a hipótese de R ser um domínio, pelo fato de R ser Noetheriano à direita. Podemos ainda supor, apenas, que R satisfaz a condição de cadeia ascendente (*c.c.a.*) sobre os anuladores principais à direita. Vamos omitir essas demontrações com o objetivo de não tornar o texto muito extenso.

Em ([17], Teorema 2) E. C. Posner afirma que se um anel de cadeia à direita R satisfaz a (*c.c.a.*) ou a (*c.c.d.*) sobre os anuladores à direita então o radical primo $\beta(R)$ de R é igual ao conjunto $T(R)$ dos elementos nilpotentes de R e este é um ideal completamente primo de R.

O que ocorre é que a demonstração deste resultado não está completa. Para provar o resultado Posner trabalha no quociente $R/\beta(R)$ e não podemos garantir que as condições de cadeia sobre os anuladores à direita em R são herdadas pelo quociente $R/\beta(R)$. Contudo, este teorema é válido e serviu de motivação para a busca de uma prova correta. Na verdade, M. Ferrero e G. Törner demonstraram um resultado mais geral que é o seguinte

Teorema 3.3. ([5], Teorema 8) *Seja R um anel distributivo à direita que possui ao menos um ideal completamente primo contido no radical de Jacobson, $J(R)$, e satisfaz a condição de cadeia ascendente (c.c.a) ou a condição de cadeia descendente (c.c.d) sobre os anuladores principais à direita. Então o radical primo $\beta(R)$ de R, é igual ao ideal singular à direita $Z(R)$ de R, e é completamente primo e nilpotente.*

Para demonstrar o teorema, vamos precisar de alguns lemas:

Lema 3.4. *Seja R um anel que satisfaz a (c.c.a.) sobre os anuladores principais à direita. Então $Z(R)$ é T-nilpotente à direita. Em particular, temos que $Z(R) \subseteq \beta(R)$.*

Demonstração: Suponhamos, por contradição, que $(x_i)_{i\in\mathbb{N}}$ é uma seqüência de elementos em $Z(R)$ tal que $x_n \dots x_2 x_1 \neq 0$ para todo $n \in \mathbb{N}$. É trivial

que $d_R(x_1) \subseteq d_R(x_2x_1) \subseteq \ldots$ Então, por hipótese, existe $m \in \mathbb{N}$ tal que $d_R(x_m b) = d_R(b)$, com $b = x_{m-1} \ldots x_1$. Agora, x_m está em $Z(R)$ e $b \neq 0$. Assim, $d_R(x_m) \cap bR \neq 0$ e existe $y \in R$ com $by \neq 0$, $x_m by = 0$, o que é uma contradição. A prova do lema está completa, tendo em vista que todo ideal que é T-nilpotente à direita está contido no radical primo $\beta(R)$, de acordo com o Teorema 1.3. □

Nos resultados a seguir diremos que o anel R satisfaz à condição (C) quando valer a seguinte afirmação:

(C) *Existe um ideal completamente primo Q de R contido no radical de Jacobson $J(R)$ de R.*

Exemplo 3.5. ([14], Exemplo 3.6) Seja $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}, b \in \mathbb{Q} \right\}$. Observe que o conjunto $K = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Q} \right\}$ é um ideal do anel R e $R/K \simeq \mathbb{Z}$. Logo, K é um ideal completamente primo de R e R/K é um anel distributivo (à direita). Observe também que o nil radical generalizado $N_g(R)$ de R é igual a K e portanto K é um ideal completamente primo de R contido no radical de Jacobson $J(R)$. Além disso, é fácil ver que os ideais de R contidos em K são $\mathbb{Z}$-submódulos de $\mathbb{Q}$. Assim, de acordo com o Exemplo 2.13, $\mathbb{Q}_{\mathbb{Z}}$ é um módulo distributivo. Logo, os ideais de R contidos em K formam um reticulado distributivo. Visto que, $I \subseteq K$ ou $K \subseteq I$ para qualquer ideal I de R, segue que R é um anel distributivo (à direita).

Exemplo 3.6. ([4], Exemplo 4.1) Seja A um domínio distributivo à direita e σ um monomorfismo de A. Então, utilizando ([20], Proposição 3.3(ii)) temos que o "skew"corpo de frações F de A existe e o reticulado de A-submódulos de F é distributivo. Denotemos também por σ a extensão de σ a um monomorfismo de F e por $F[[t;\sigma]]$ o "skew"anel de série de potências definido por $at = ta^\sigma$ para qualquer $a \in F$.

Seja $R = A \oplus tF[[t;\sigma]]$. Em ([4], Exemplo 4.1) os autores mostram que se $I <_d R$, então $I = (I \cap A) \oplus tF[[t;\sigma]]$. Assim, temos que o radical de Jacobson de R é $J(R) = J(A) \oplus tF[[t;\sigma]]$. Além disso, os autores também mostram que se $H <_d R$, então $H = t^n H_0 + t^{n+1} F[[t;\sigma]]$ onde $H_0 = \{a \in F : t^n a \in H\}$ é um

A-submódulo de F. Como o reticulado de A-submódulos de F é distributivo segue que R é distributivo à direita. Se tomarmos por exemplo, $A = \mathbb{Z}$, temos $J(A) = 0$ e, então, $J(R) = tF[[t;\sigma]]$ e este ideal é completamente primo de R porque $R/J(R) \simeq \mathbb{Z}$.

O próximo lema será composto de alguns resultados que são encontrados em ([20], Proposição 2.1(ii)) e ([14], Lema 3.1(i), Lema 3.1(ii), Teorema 3.2, Corolário 3.3 e Teorema 3.4).

Lema 3.7. *Seja R um anel distributivo à direita e Q um ideal completamente primo contido em $J(R)$. Então:*

(i) *Para cada ideal à direita I de R, temos $I \subseteq Q$ ou $Q \subseteq I$.*

(ii) *Se $r \in R \setminus Q$ então $Q = rQ$.*

(iii) *Para quaisquer $a, b \in R$ temos: os elementos a, b são comparáveis no seguinte sentido, $aR \subseteq bR$ ou $bR \subseteq aR$, ou $aQ = bQ$.*

(iv) *Se I é um ideal de R não nilpotente tal que $I \subseteq Q$ então a intersecção $\bigcap_{n\in\mathbb{N}} I^n$ é um ideal completamente primo de R.*

(v) *O radical primo $\beta(R)$ de R é um ideal primo.*

(vi) *Não existe ideal I de R com $\beta(R) \subset I \subset N_g(R)$.*

Demonstração: (i) Suponhamos que $I \nsubseteq Q$ e seja $a \in I$ tal que $a \notin Q$. Então, para qualquer $q \in Q$, $\{x \in R : ax \in qR\} \subseteq Q$. Pela Observação 2.19, temos $\{x \in R : ax \in qR\} + \{y \in R : qy \in aR\} = R$. Entretanto, $\{x \in R : ax \in qR\} \subseteq Q$. Logo, $Q + \{y \in R : qy \in aR\} = R$. Então, podemos escrever $1 = q' + y'$ para algum $q' \in Q$ e algum $y' \in \{y \in R : qy \in aR\}$. Equivalentemente, $1 - q' = y'$. Como $Q \subseteq J(R)$ por hipótese, $q' \subseteq J(R)$. Logo, $1 - q' = y'$ é invertível em R. Portanto, existe um elemento invertível no ideal à direita $\{y \in R : qy \in aR\}$, o que implica $\{y \in R : qy \in aR\} = R$. Conseqüentemente, $q \in aR \subseteq I$. Portanto, $Q \subseteq I$.

(ii) Utilizando a parte (i) e o fato de que $r \notin Q$, temos que $Q \subseteq rR$. Seja $q \in Q$. Então existe $x \in R$ com $q = rx$. Mas Q é completamente primo, $r \notin Q$ e $q \in Q$. Logo, $x \in Q$. Então, $q \in rQ$, isto é, $Q \subseteq rQ$. A outra inclusão é óbvia. Portanto, $Q = rQ$.

(iii) Suponhamos que $aR \nsubseteq bR$ e $bR \nsubseteq aR$. Pelo Teorema 2.18, existem $x, y \in R$ com $x + y = 1$, $ax \in bR$ e $by \in aR$. Se $y \in J(R)$ então $x = 1 - y$ é um invertível de R e obtemos $a \in bR$, o que é uma contradição. Desta forma, $y \notin J(R)$ e conseqüentemente, $y \notin Q$. Agora, (ii) implica $bQ = byQ \subseteq aQ$. De forma análoga, utilizando a hipótese de $bR \nsubseteq aR$ chegamos em $aQ \subseteq bQ$.

(iv) Suponhamos, por contradição, que existem $a, b \notin \bigcap_{n\in\mathbb{N}} I^n$ tais que $ab \in \bigcap_{n\in\mathbb{N}} I^n$. Então $a, b \notin I^n$ para algum natural n. Seja $x \in I^n$. Visto que $aR \nsubseteq xR$ e $bR \nsubseteq xR$, a parte (iii) do lema implica $xI^n \subseteq xQ \subseteq aQ \cap bQ$. Desta forma, $I^{2n} \subseteq aQ \cap bQ$ e agora, $I^{4n} = I^{2n}I^{2n} \subseteq aQI^{2n} \subseteq aI^{2n} \subseteq abQ$. Visto que $ab \in I^{4n}$, $ab = abq$ para algum $q \in Q$. Mas, $Q \subseteq J(R)$. Assim, $q \in J(R)$ e, conseqüentemente $1 - q$ é invertível. Segue que $ab = 0$. Logo, $I^{4n} = 0$ e I é nilpotente, o que é uma contradição.

(v) Observe inicialmente que, da parte (i) do lema, temos o seguinte resultado

A condição (C) é satisfeita em um anel distributivo à direita se, e somente se, o nil radical generalizado $N_g(R)$ de R é completamente primo.

De fato, se valer a condição (C), utilizando a parte (i) deste lema, concluímos que os ideais completamente primos de R, contidos em $J(R)$ formam uma cadeia. Logo, é de fácil verificação que $N_g(R)$ é um ideal completamente primo. Reciprocamente, do Corolário 2.25, temos que $N_g(R) \subseteq J(R)$ isto é, vale a condição (C).

Agora, se $N_g(R) = \beta(R)$, então obviamente $\beta(R)$ é primo. Suponhamos que $\beta(R) \subset N_g(R)$. Visto que $N_g(R)$ é completamente primo, qualquer ideal de R é comparável com $N_g(R)$ pela parte (i) do lema. Conseqüentemente, $P \subset N_g(R)$ para algum ideal primo P de R. Agora, da parte (iv) do lema segue que P é nilpotente e assim, $P \subseteq \beta(R)$. Desta forma, $\beta(R) = P$ e conseqüentemente, $\beta(R)$ é primo.

(vi) Suponhamos, por contradição, que existe um ideal $0 \neq I \lhd R$ com $\beta(R) \subset I \subset N_g(R)$. Logo, I é um ideal não nilpotente e, por (iv), $\bigcap_{n\in\mathbb{N}} I^n$ é um ideal completamente primo de R. Então, $N_g(R) \subseteq \bigcap_{n\in\mathbb{N}} I^n \subset N_g(R)$ o que é uma contradição. □

Proposição 3.8. *Seja R um anel distributivo à direita que satisfaz a condição (C). Então R é um anel não singular à direita se, e somente se, é um domínio.*

Demonstração: Suponhamos que $Z(R) = 0$ e seja Q um ideal completamente primo de R contido em $J(R)$. Se Q é igual a zero não há nada a fazer. Assim, suponhamos $Q \neq 0$. Tome quaisquer elementos não-nulos $a, b \in R$. Pelo Lema 3.7 (iii), nós temos as alternativas $aR \subseteq bR$, $bR \subseteq aR$ ou $aQ = bQ$. Inicialmente, vamos considerar o caso $aQ = bQ$. Se $aQ = 0$ então $d_R(a) \supseteq Q$ e, pelo Lema 3.7 (i), e o fato de $Q \neq 0$, $d_R(a)$ é um ideal à direita essencial de R. Conseqüentemente, $a \in Z(R) = 0$ o que é uma contradição com o fato de a ser não-nulo. Logo, $aQ = 0$ não pode acontecer. Se $aQ \neq 0$ segue que $aR \cap bR \neq 0$ pois $aQ = bQ$. Se ocorrer uma das outras alternativas, isto é, $aR \subseteq bR$ ou $bR \subseteq aR$, temos também que $aR \cap bR \neq 0$ pois a e b são não-nulos. Logo, em qualquer um dos casos em que não ocorreu contradição temos $aR \cap bR \neq 0$, onde a e b são quaisquer elementos não-nulos de R. Então, pela Observação 1.15, segue que qualquer ideal à direita não nulo de R é essencial. Logo, pela Proposição 1.19, $Z(R) = 0$ é um ideal completamente primo de R e, portanto, R é um domínio. A outra implicação é óbvia. □

Lema 3.9. *Seja R um anel distributivo à direita. Então $R/Z(R)$ não possui elementos nilpotentes não nulos.*

Demonstração: Suponhamos que $a \notin Z(R)$ e $a^2 \in Z(R)$. Conseqüentemente, $H = d_R(a^2)$ é um ideal à direita essencial de R e $L = d_R(a)$ não é essencial. Assim, existe um ideal à direita não nulo B de R com $L \cap B = 0$ e, então, $L \cap (H \cap B) = 0$. Pela Proposição 2.17, temos que $Hom_R(H \cap B, L) = 0$ e visto que $a(H \cap B) \subseteq L$, nós obtemos $a(H \cap B) = 0$. Logo, $H \cap B \subseteq d_R(a) = L$ e, conseqüentemente $H \cap B = 0$, o que é uma contradição. □

Veremos agora, alguns lemas que serão necessários para o caso de $(c.c.d.)$.

Lema 3.10. *Seja R um anel distributivo à direita que satisfaz a condição (C). Se I é um ideal de R com $N_g(R) \nsubseteq I$, então temos $I \subseteq \beta(R)$.*

Demonstração: Pelo Lema $3.7\,(i)$, $I \subset N_g(R)$. Conseqüentemente, se $N_g(R) = \beta(R)$ não há nada a fazer. Vamos assumir então que $\beta(R) \subset N_g(R)$. Suponhamos, por absurdo, que existe $a \in I$ com $a \notin \beta(R)$ e tomemos $b \in \beta(R)$. Pelo Lema $3.7\,(iii)$, uma das três condições seguintes irá ocorrer: $(i)\ a \in bR \subseteq \beta(R)$, $(ii)\ aN_g(R) = bN_g(R) \subseteq \beta(R)$ ou $(iii)\ b \in aR \subseteq I$. A primeira condição é um absurdo pois $a \notin \beta(R)$. A segunda está em contradição com o fato de $\beta(R)$ ser primo. A última possibilidade implica $\beta(R) \subseteq I \subset N_g(R)$ e assim, pelo Lema $3.7\,(vi)$, $I = \beta(R)$. Isto é uma contradição com a hipótese de existir $a \in I$ tal que $a \notin \beta(R)$. Desta forma, $I \subseteq \beta(R)$. □

Lema 3.11. *Seja R um anel distributivo à direita e Q um ideal completamente primo contido em $J(R)$. Então $Q^2 = \{ab : a, b \in Q\}$.*

Demonstração: Por indução, é suficiente provar que se $x = a_1b_1 + a_2b_2 \in Q^2$ com $a_i, b_i \in Q$ e $i = 1, 2$, então existem $a, b \in Q$ tais que $x = ab$. Pelo Lema $3.7\,(iii)$, nós temos que $a_1 = a_2y$ ou $a_2 = a_1y$, para algum $y \in R$, ou ainda $a_1Q = a_2Q$. Se $a_1 = a_2y$, então $x = a_1b_1 + a_2b_2 = a_2yb_1 + a_2b_2 = a_2(yb_1 + b_2)$. Note que $(yb_1 + b_2) \in Q$ e portanto, x é o produto de dois elementos de Q. Se $a_2 = a_1y$ a demonstração é análoga. No último caso, $a_1b_1 = a_2b'$, para algum $b' \in Q$. Então, $x = a_2b' + a_2b_2 = a_2(b' + b_2)$. Como $(b' + b_2) \in Q$, o lema está demonstrado. □

Lema 3.12. *Seja R um anel distributivo à direita e Q um ideal completamente primo de R contido em $J(R)$. Além disso, suponhamos que R satisfaz a (c.c.d.) sobre os anuladores principais à direita. Então nós temos:*

(i) $Z(R) \subseteq Q$

(ii) *Se* $Q = Q^2 \neq 0$, *então* $Z(R) \subset Q$.

Demonstração: (i) Se $Q = 0$, então R é um domínio e $Z(R) = 0$. Considere então, $Q \neq 0$. Suponhamos $Q \subset Z(R)$ e sejam $a \in Z(R)$, $a \notin Q$ e $0 \neq b \in Q$. Pelo Lema $3.7(ii)$, nós temos $Q = aQ$. Conseqüentemente, existe $c \in Q$ tal que $b = ac$. Assim, $d_R(c) \subseteq d_R(b)$ e $d_R(a) \cap cR \neq 0$. Desta forma, existe $x \in R$ com $cx \neq 0$ e $acx = 0$, que implica $d_R(c) \subset d_R(b)$. Com este mesmo raciocínio e iniciando com c ao invés de b, nós obtemos

uma seqüência $d_R(c) \supset d_R(c_1) \supset d_R(c_2) \supset \ldots$ o que é uma contradição com a (*c.c.d.*). Logo, $Z(R) \subseteq Q$, pelo Lema 3.7 (i).

(ii) Suponhamos $Q = Z(R)$ e tomemos qualquer elemento $0 \neq a \in Q$. Por hipótese, $a = bc$ para certos $b, c \in Q$, (utilizando o Lema 3.11). Conseqüentemente, $d_R(c) \subseteq d_R(a)$, e com os mesmos argumentos usados em (i), podemos concluir que $d_R(c) \subset d_R(a)$. Isso leva novamente a uma contradição como em (i). Portanto, $Z(R) \subset Q$. □

Estamos agora em condições de provar o Teorema 3.3.

Demonstração do Teorema 3.3: Caso 1. Suponhamos que R satisfaz a (*c.c.a.*) sobre os anuladores principais à direita. Então, pelo Teorema 1.18, $R/\beta(R)$ é um anel não singular à direita. Além disso, como R satisfaz a condição (C), é fácil ver que $R/\beta(R)$ também satisfaz (C). Pelo Corolário 2.11, segue que $R/\beta(R)$ é distributivo à direita. Então $\beta(R)$ é completamente primo pela Proposição 3.8. Também, $Z(R) = \beta(R)$ pelos Lemas 3.4 e 3.9. Finalmente, pelo Lema 3.7(iv), nós temos que $\beta(R)$ é, ou nilpotente, ou $\beta(R) = \big(\beta(R)\big)^2 \neq 0$. Suponhamos que $\beta(R) = \big(\beta(R)\big)^2 \neq 0$ e tomemos $0 \neq a \in \beta(R)$. Então existem $a_1, b_1 \in \beta(R)$ com $a = a_1 b_1$. Repetindo o argumento, iniciando com a_1 em vez de a, nós temos $a = a_2 b_2 b_1$ para $a_2, b_2 \in \beta(R)$. Por indução, obtemos a seqüência $\{b_1, b_2, \ldots\}$ de elementos de $\beta(R)$ tais que para cada $m \geq 1$, existe $a_m \in \beta(R)$ com $a = a_m b_m \ldots b_1$. Por outro lado, $\beta(R) = Z(R)$ é T-nilpotente à direita e, assim, obtemos $a = 0$, o que é uma contradição.

Caso 2. Suponhamos que R satisfaz a (*c.c.d.*) sobre os anuladores principais à direita. Visto que o nil radical generalizado $N_g(R)$ é completamente primo, $Z(R) \subseteq N_g(R)$ pelo Lema 3.12. Assim, $Z(R) \subseteq \beta(R)$ se $N_g(R) = \beta(R)$. Se $N_g(R) \neq \beta(R)$, nós temos $N_g(R) = \big(N_g(R)\big)^2 \neq 0$ de acordo com o Lema 3.7 (vi). Isso implica $Z(R) \subset N_g(R)$ pelo Lema 3.12. E então, pelo Lema 3.10, $Z(R) \subseteq \beta(R)$ em qualquer um dos casos. Logo, utilizando o Lema 3.9, $\beta(R) = Z(R)$ e $R/\beta(R)$ é um anel primo que não possui elementos nilpotentes não nulos. Logo, $\beta(R)$ é completamente primo. Finalmente, se $\beta(R)$ não é nilpotente, como no caso 1 nós obtemos $\beta(R) = \big(\beta(R)\big)^2 \neq 0$. Assim, $Z(R) \subset \beta(R)$ o que é uma contradição. □

Corolário 3.13. *Seja R um anel distributivo à direita que satisfaz a condição (C) e a (c.c.a.) sobre os anuladores principais à direita. Então, $\beta(R) = N_d(R)$ onde $N_d(R)$ é o conjunto dos divisores de zero à direita de R.*

Demonstração: Obviamente, $\beta(R) \subseteq N_d(R)$. Para mostrar a outra inclusão, suponhamos por absurdo que existe $a \in N_d(R)$ tal que $a \notin \beta(R)$ ou, de forma equivalente, $d_R(a) \neq 0$ e $a \notin \beta(R)$. Conseqüentemente, $d_R(a) \subseteq d_R(a^2) \subseteq \ldots$ e $a^n \notin \beta(R)$ para qualquer inteiro n, visto que $\beta(R)$ é completamente primo. Por hipótese, existe m tal que $d_R(a^m) = d_R(a^{m+1})$. Tomemos qualquer $0 \neq b \in d_R(a)$. Desta forma, $ab = 0$ e, então, segue que $b \in \beta(R) \subset a^m R$. Logo, $b = a^m x$ para algum $x \in R$. Assim, $a^{m+1}x = 0$, o que nos leva a $b = a^m x = 0$, que é uma contradição. □

Vamos encerrar o trabalho com o Teorema de Posner que comentamos anteriormente e que passa a ser uma conseqüência do Teorema 3.3:

Corolário 3.14. ([17], Teorema 2) Seja R um anel de cadeia à direita que satisfaz a (*c.c.a.*) ou a (*c.c.d.*) sobre os anuladores à direita. Então o radical primo $\beta(R)$ de R é igual ao conjunto $T(R)$ dos elementos nilpotentes de R e é um ideal completamente primo de R.

Demonstração: De acordo com a Proposição 1.27, pelo fato de R ser um anel de cadeia à direita, R é um anel distributivo à direita. Além disso, R é um anel local e o único ideal à direita maximal é exatamente o radical de Jacobson $J(R)$. Pelo Corolário 2.25, $J(R)$ é um ideal (bilateral) completamente primo. Logo, utilizando o Teorema 3.3 segue que o radical primo $\beta(R)$ de R é completamente primo. No Capítulo 1, vimos que $\beta(R)$ é um nil ideal de R, então $\beta(R) \subseteq T(R)$.

Reciprocamente, se x é um elemento nilpotente de R, existe $n \in \mathbb{N}$ tal que $x^n = 0 \in \beta(R)$. Mas, $\beta(R)$ é completamente primo pelo que concluímos acima. Então, $x \in \beta(R)$ e portanto, $\beta(R) = T(R)$. □

Referências Bibliográficas

[1] Birkhoff, G., *"Lattice Theory"*, Colloquium Publications, Volume XXV, American Mathematical Society, 1948.

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

[3] Ferrero, M. and Sant'Ana, A., *"Rings with comparability"*, Canad. Math. Bull. 42(2) (1999), 174-183.

[4] Ferrero, M. and Törner, G., *"On Waists of right distributive rings"*, Forum Math. 7 (1995), 419-433.

[5] Ferrero, M. and Törner, G., *"Rings with annihilator chain conditions and right distributive rings"*, Proc. Amer. Math. Soc. 119 (1993), 401-405

[6] Ferrero, M., *"Atas da XVI Escola de Álgebra - Parte III"*, Universidade de Brasília, Instituto de Ciências Exatas - Departamento de Matemática, 23 a 29 de julho de 2000.

[7] Gardner, B.J., *"Some aspects of T-nilpotence"*, Pacific J. Math. 53 (1974), 117-130.

[8] Gericke, H., *"Lattice Theory"*, Frederick Ungar Publishing Co , New York, 1966.

[9] Goodearl, K.R., *"Ring Theory - Nonsingular Rings and Modules"*, Monographs and Textbooks in Pure and Applied Mathematics, Marcel Dekker, Inc., New York - Basel, 1976.

[10] Johns, B., *"Chain conditions and nil ideals,"*, J. Algebra 73 (1981), 287-294.

[11] Lam, T.Y., *"A First Course in Noncommutative Rings"*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1991.

[12] Lam, T.Y., *"Lectures on Modules and Rings"*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1998.

[13] Lambek, J., *"Lectures on Rings and Modules"*, McGill University, Chelsea Publishing Company, 2nd Edition, New York, 1976.

[14] Mazurek, R., *"Distributive rings with Goldie dimension one"*, Comm. Algebra 19 (1991), 931-944.

[15] Mazurek, R., *"An Introduction to Distributive Rings and Modules"*, Universidade Federal do Rio Grande do Sul - Instituto de Matemática, Cadernos de Matemática e Estatística, Série F, Número 15: Trabalho de Divulgação, 2003.

[16] Mazurek R. and Puczylowski E. R., *"On nilpotents elements of distributive rings"*, Comm. Algebra 18 (1990), 463-471.

[17] Posner, E.C., *"Left valuation rings and simple radical rings"*, Trans. Amer. Math. Soc. 107 (1963), 458-465.

[18] Rutherford, D.E., *"Introduction to Lattice Theory"*, University Mathematical Monographs, Oliver and Boyd, 1965.

[19] Stenström, B., *"Rings of Quotients"*, Springer-Verlag, Berlin - Heidelberg - New York, 1975.

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

[21] Tuganbaev, A., *"Distributive Modules and Related Topics"*, Gordon and Breach, Science Publishers, Amsterdam, 1999.