Universidade Federal do Rio Grande do Sul

Instituto de Matemática
Programa de Pós-Graduação em Matemática

SOBRE O GRAU DE DISTRIBUTIVIDADE DE ANÉIS E MÓDULOS

Dissertação de Mestrado

FELIPE LOPES CASTRO

Porto Alegre, 28 de março de 2011

Dissertação submetida por Felipe Lopes Castro[1], como requisito parcial para obtenção do grau de Mestre em Ciências Matemáticas, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Prof. Dr. Alveri Alves Sant'Ana (PPG-Mat/UFRGS)

Banca Examinadora:

Prof. Dr. Miguel A. A. Ferrero (PPG-Mat/UFRGS)

Prof^a. Dr^a. Luisa R. Döering (PPG-Mat/UFRGS)

Prof. Dr. João R. Lazzarin (PPG-Mat/UFSM)

[1]Bolsista da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Agradecimentos

Gostaria de agradecer à minha esposa, Erica, por todo carinho e dedicação, ao meu filho, Henri, pelos sorrisos e fraldas recheadas, aos meus pais pela confiança e incentivo, e à toda minha família.

Agradeço ao meu orientador, Alveri, pelos conselhos, pela compreensão e paciência, durante a graduação, mestrado e agora no doutorado, ao Paques, pelas divertidas aulas, ao Programa de Pós-Graduação em Matemática desta Universidade. Agradeço aos professores da banca, pelas recomendações e críticas.

Agradeço aos meus amigos da Pós, em especial ao Rene, à Andrea e ao Di, pelos momentos especiais durante estes dois anos, pelas conversas na sala do cafézinho, e pelas cópias dos cadernos da Déia.

Dedico esta dissertação ao meu lindo filho, Henri
Ferreira Castro, que me tornou um homem mais
responsável e feliz.

RESUMO

Este trabalho tem por objetivo estudar o grau de distributividade de módulos e anéis, em especial, o caso de um anel de matrizes. Estudaremos módulos e anéis distributivos, apresentando alguns resultados de Stephenson [11] e de Ferrero e Sant'Ana [3]. Estenderemos uma caracterização de distributividade para ω-distributividade, onde ω é um cardinal qualquer ([3], Teorema 1.1). Finalmente, calcularemos o grau de distributividade de um anel de matrizes.

ABSTRACT

The purpose of this work is to study the distributive degree of modules and rings, specially the matrix ring case. We will study distributive modules and rings, presenting some results of Stephenson [11] and of Ferrero and Sant'Ana [3]. We extend a characterization of distributivity to ω-distributivity ([3], Theorem 1.1). Finally, we compute the distributivity degree of a matrix ring.

Sumário

Introdução

Neste trabalho estudamos anéis e módulos distributivos. Um R-módulo à direita M é dito *distributivo* se o seu reticulado de submódulos, $\mathcal{L}_R(M)$, é distributivo, isto é, dados quaisquer I, J, K submódulos de M, temos $I \cap (J + K) = (I \cap J) + (I \cap K)$. De maneira análoga, um anel R é dito *distributivo à direita (resp. à esquerda)* se o seu reticulado de ideais à direita (resp. à esquerda) é distributivo.

A noção de distributividade é estendida para ω-distributividade da seguinte maneira: sejam $\omega \geq 2$ um cardinal, Ω um conjunto de cardinalidade ω e M um R-módulo à direita. Então M é dito *ω-distributivo* se o seu reticulado de submódulos é ω-distributivo, isto é, para qualquer submódulo N e qualquer família de submódulos $(N_i)_{i\in\Omega}$ de M temos $N + \bigcap_{i\in\Omega} N_i = \bigcap_{i\in\Omega}(N + \bigcap_{j\neq i} N_j)$. Um anel R é dito *ω-distributivo à direita (resp. à esquerda)* se R_R (resp. ${}_RR$) é ω-distributivo. Observemos que, os módulos distributivo são exatamente os módulos 2-distributivos, e que um módulo ω-distributivo é ω'-distributivo, para todo $\omega' \geq \omega$.

O *grau de distributividade* de um R-módulo à direita M é o menor cardinal α tal que M é α-distributivo. O grau de distributividade à direita (resp. à esquerda) de um anel R é o menor cardinal α tal que R é α-distributivo à direita (resp. à esquerda). O objetivo deste trabalho é calcular o grau de distributividade de certos anéis, em especial do anel de matrizes. Para isso, começaremos estudando reticulados e depois, apresentaremos uma caracterização de anéis e módulos distributivos que provém da tradução de uma caracterização de reticulados distributivos, para a linguagem de anéis e módulos. Estenderemos, a seguir, estes resultados para o caso de ω-distributividade. Por fim, introduziremos o grau de distributividade e calcularemos este grau para o caso de um anel de matrizes.

Stephenson publicou, em 1974, o primeiro trabalho importante sobre distributividade [11], a partir do qual, muitos outros se seguiram. Alguns resultados de Stephenson serão apresentados aqui. Ferrero e Sant'Ana, em [3] (2003), estudaram ω-distributividade e introduziram o conceito de grau de distributividade de anéis e módulos, trabalho no qual os dois últimos capítulos desta dissertação são baseados.

No primeiro capítulo apresentaremos conceitos básicos da teoria de anéis e módulos, os quais serão importantes para o bom entendimento desta dissertação. Neste sentido, são tratados aqui ideais primos, radical de Jacobson e a construção do anel de frações, bem como do módulo de frações.

No segundo capítulo estudaremos reticulados, em especial os reticulados distributivos. Mostramos (Teorema 2.2.9) que um reticulado modular é distributivo se, e somente se, complementos relativos são únicos.

No terceiro capítulo, estudamos módulos distributivos baseados no artigo de Stephenson [11] e no artigo de Ferrero e Sant'Ana [3]. O principal resultado desta seção é o Teorema 3.2.24, que caracteriza R-módulos distributivos a partir do seu reticulado dos R-submódulos S_P-saturados, onde $S_P = R \backslash P$ e $P \in \mathcal{M}ax_r(R)$, sendo que $\mathcal{M}ax_r(R)$ denota o conjunto dos ideais à direita maximais de R.

No quarto capítulo estudaremos ω-distributividade, com base no artigo [3], tendo como principal resultado o Teorema 4.1.2, o qual caracteriza ω-dis-

tributividade. Finalmente, discutimos o grau de distributividade de anéis e módulos e mostramos, por exemplo, que o grau de distributividade à direita de $\mathcal{M}_n(R)$ é $n+1$, quando R é um domínio distributivo e comutativo.

Capítulo 1

Pré-requisitos

Neste capítulo abordaremos alguns tópicos básicos necessários ao desenvolvimento da teoria que se segue. Em todo caso, é esperado do leitor alguma familiaridade com teoria de anéis e módulos.

Neste trabalho os anéis considerados são unitários e, em geral, não-comutativos e denotados por R. O conjunto dos elementos invertíveis de R será denotado por $\mathcal{U}(R)$. Consideraremos, a menos que seja dito algo em contrário, todo módulo como sendo um R-módulo à direita. Os ideais à esquerda ou à direita, I, de R serão denotados, respectivamente, por $I \triangleleft_l R$ e $I \triangleleft_r R$, e um ideal bilateral J de R será chamado apenas de ideal de R e denotado por $J \triangleleft R$. O conjunto dos ideais à direita maximais de R será denotado por $\mathcal{M}ax_r(R)$.

1.1 Ideais Primos

Nesta seção apresentaremos algumas propriedades importantes sobre a primalidade de ideais, propriedades estas que serão importantes posteriormente.

Definição 1.1.1. Um ideal à direita P de R, $P \neq R$, é dito:

1. *primo*, se para quaisquer ideais à direita A, B de R tais que $AB \subseteq P$, tivermos $A \subseteq P$ ou $B \subseteq P$;

2. *semiprimo*, se para qualquer ideal à direita A de R tal que $A^2 \subseteq P$, tivermos $A \subseteq P$;

3. *completamente primo*, se para quaisquer $a, b \in R$ tais que $ab \in P$, tivermos $a \in P$ ou $b \in P$;

4. *completamente semiprimo*, se para qualquer $a \in R$ tal que $a^2 \in P$, tivermos $a \in P$.

Observação 1.1.2. A partir das definições acima:

1. Fica claro que um ideal P de um anel R é completamente primo se, e somente se, R/P é um domínio.

2. Também, um anel R é dito *primo (resp. semiprimo)* se o ideal nulo é primo (resp. semiprimo).

Os próximos resultados caracterizam ideais primos e semiprimos.

Proposição 1.1.3. *Seja P um ideal à direita de R, $P \neq R$. Então P é um ideal à direita primo se, e somente se, para quaisquer $a, b \in R$ tais que $aRb \subseteq P$, tivermos $a \in P$ ou $b \in P$.*

Demonstração. Suponhamos que P seja um ideal primo de R. Sejam $a,\ b \in R$ tais que $aRb \subseteq P$ e suponhamos que $b \notin P$. Como $aRbR \subseteq PR \subseteq P$ e P é um ideal à direita primo, então temos que $aR \in P$ ou $bR \in P$. Como $b \notin P$, logo $bR \nsubseteq P$. Portanto $aR \subseteq P$ e, consequentemente, $a \in P$.

Reciprocamente, suponhamos que para quaisquer $c,\ d \in P$ tais que $cRd \subseteq P$ temos $c \in P$ ou $d \in P$. Sejam $A,\ B$ ideais à direita não-nulos de R tais que $AB \subseteq P$ e suponhamos que $B \not\subseteq P$. Seja $b \in B \backslash P$. Então para todo $a \in A$, temos $aRb \subseteq P$ e, consequentemente $a \in P$, pois $b \notin P$. Portanto $A \subseteq P$. $\square$

Proposição 1.1.4. *Seja P um ideal à direita próprio de R. Então P é um ideal à direita semiprimo se, e somente se, para qualquer $a \in R$, tal que $aRa \subseteq P$, temos $a \in P$.*

Demonstração. Suponhamos que P seja um ideal semiprimo e seja $a \in R$ tal que $aRa \subseteq P$. Então $aRaR \subseteq PR \subseteq P$. Como P é um ideal semiprimo de R, então $aR \subseteq P$ e, portanto, $a \in P$.

Reciprocamente, suponhamos que para qualquer $r \in R$ tal que $rRr \subseteq P$ temos $r \in P$. Seja A um ideal à direita de R tal que $A^2 \subseteq P$ e tomamos $a \in A$ qualquer. Então $aRa \subseteq P$ e, por hipótese, $a \in P$. Portanto $A \subseteq P$. $\square$

1.2 O Radical de Jacobson

Nesta seção, definiremos o radical de Jacobson de um anel R e de um R-módulo à direita M, e veremos algumas propriedades importantes para o desenvolvimento deste trabalho.

Definição 1.2.1. O *radical de Jacobson* de um anel R, $J(R)$, é a intersecção dos ideais à direita maximais de R.

Pelo Lema de Zorn, sabemos que todo anel unitário R possui ideais maximais. Apesar de termos definido o radical de Jacobson como a intersecção de uma família de ideais à direita, mais adiante veremos que $J(R)$ é um ideal bilateral de R, sendo desnecessário qualquer denominação de lateralidade.

Agora vamos mostrar uma caracterização de $J(R)$ à nível de elementos. Primeiramente precisamos definir o que é um módulo simples.

Definição 1.2.2. Um R-módulo à direita $M \neq 0$ é dito *simples*, se os únicos submódulos de M são 0 e M. Analogamente, um anel R é dito *simples*, se os seus únicos ideais são 0 e R.

Observamos que se R é um anel qualquer e $\mathcal{M}$ é um ideal à direita maximal de R, então $R/\mathcal{M}$ é um R-módulo simples.

Proposição 1.2.3. *Seja R um anel e $a \in R$. Então são equivalentes as seguintes afirmações:*

1. $a \in J(R)$*;*

2. $1 - ab$ *é invertível à direita, para todo* $b \in R$*;*

3. $Ma = 0$*, para qualquer* R*-módulo à direita simples* M*.*

Demonstração. (1) $\Rightarrow$ (2)

Seja $a \in J(R)$ e suponhamos que para algum $b \in R$, $1 - ab$ não seja invertível, então $(1 - ab)R$ está contido em algum ideal à direita maximal A de R. Logo $1 - ab \in A$, mas como $a \in J(R) \subseteq A$, então temos que $1 \in A$, o que é uma contradição. Portanto $1 - ab$ é invertível, para todo $b \in R$.

(2) $\Rightarrow$ (3)

Suponhamos que exista um R-módulo à direita simples M tal que $Ma \neq 0$, logo existe $m \in M$ tal que $ma \neq 0$. Mas como M é simples, então $maR = M$. Logo existe $b \in R$ tal que $mab = m$, ou seja, $m(1 - ab) = 0$. Como, por hipótese, $1 - ab$ é invertível, segue que $m = 0$, o que é uma contradição.

(3) $\Rightarrow$ (1)

Para todo ideal à direita maximal $\mathcal{M}$ de R, $R/\mathcal{M}$ é um R-módulo à direita simples. Logo $(R/\mathcal{M})a = 0$, e $a \in \cap\{\mathcal{M} \triangleleft_r R | \ \mathcal{M} \text{ maximal } \} = J(R)$. $\square$

Corolário 1.2.4. *O radical de Jacobson de um anel é um ideal bilateral.*

Demonstração. Seja $J(R)$ o radical de Jacobson de um anel R, então claramente $J(R)$ é um ideal à direita. Sejam $a \in J(R)$ e $r \in R$. Vamos mostrar que $1-(ra)b$ tem inverso à direita, para todo $b \in R$. Como $J(R)$ é um ideal à direita, então $ab \in J(R)$, para todo $b \in R$. Logo, basta mostrar que $(1-ra) \in J(R)$. Como $a \in J(R)$, pela proposição anterior, temos que $(1-ar)$ é invertível, isto é, existe $u \in R$ tal que $(1-ar)u = 1$, ou seja, $u - aru = 1$. Logo $u = 1 + aru$. Então $(1-ra)(1+rua) = 1 + rua - ra - rarua = 1 + rua - r(1+aru)a = 1 + rua - rua = 1$, portanto $ra \in J(R)$. □

Quando um anel é unitário o Lema de Zorn garante que existem ideais maximais, mas no caso de um R-módulo não há um resultado equivalente, que garanta a existência de R-submódulos maximais, então definimos o radical de Jacobson de um R-módulo qualquer da seguinte maneira.

Definição 1.2.5. Seja M um R-módulo à direita. O *Radical de Jacobson* do módulo M, denotado por $J(M)$, é a intersecção dos submódulos maximais próprios de M. Se M não possuir submódulos maximais próprios, então tomaremos $J(M) = M$.

Seja M um R-módulo à direita qualquer. Observemos agora que, se S é um R-módulo à direita simples e $f : M \to S$ um homomorfismo não-nulo de R-módulos, então $Ker\ (f)$ é um R-submódulo maximal de M, pois $M/Ker(f) \simeq S$. Portanto, segue que $\{x \in M |\ f(x) = 0,\ \forall f : M \to S,$ onde S_R é simples$\}$. Reciprocamente, se tomarmos $x \in J(M)$, então temos $x \in \bigcap\limits_{\substack{N \subseteq M \\ maximal}} N \subseteq \bigcap\limits_{\substack{f:M\to S \\ S_R \text{ simples}}} Ker(f)$. Assim, temos uma caracterização do radical de Jacobson de M dada por $J(M) = \{x \in M |\ f(x) = 0$, para todo R-homomorfismo $f : M \to S$, onde S é um R-módulo simples$\}$, o qual será usado no próximo resultado.

O lema a seguir será útil no decorrer do trabalho.

Lema 1.2.6. *Sejam R um anel e M um R-módulo à direita. Então $MJ(R) \subseteq J(M)$, para todo módulo M.*

Demonstração. Pela Proposição 1.2.3, temos que $J(R)$ anula todo R-módulo simples N. Então para todo homomorfismo não-nulo $\varphi : M \to N$ temos $0 = NJ(R) = \varphi(M)J(R) = \varphi(MJ(R))$. Pelo observado anteriormente temos $J(M) = \{x \in M | \ \psi(x) = 0, \forall \psi : M \to N$, onde N é R-módulo simples$\}$, e o resultado segue. □

1.3 Anéis de Frações

Nesta seção estamos interessados em construir o anel de frações de um anel R qualquer, para isso iniciamos observando a maneira como construímos o corpo de frações $\mathbb{Q}$ sobre $\mathbb{Z}$, em seguida construímos o anel de frações de um anel comutativo, e, por fim, fazemos a construção da situação mais geral. No final, definimos o módulo de frações, que é uma construção análoga ao anel de frações, e será útil no decorrer do trabalho.

Para a construção do corpo de frações $\mathbb{Q}$ precisamos da seguinte relação de equivalência, definida em $\mathbb{Z} \times \mathbb{Z}^\star$, onde $\mathbb{Z}^\star = \mathbb{Z} \backslash \{0\}$, dada por:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc, \ \forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^\star.$$

Assim, definimos o corpo de frações $\mathbb{Q} \simeq (\mathbb{Z} \times \mathbb{Z}^\star)/ \sim$.

Esta regra, que define a relação de equivalência, funciona muito bem para domínios em geral. Assim, para qualquer domínio D podemos definir, da mesma maneira, o corpo de frações de D. Agora veremos como generalizar esta construção para o caso de um anel comutativo, onde podemos ter divisores de zero.

1.3.1 O Caso Comutativo

Vamos agora construir o anel de frações de R (anel comutativo) em relação a um sistema multiplicativamente fechado S de R. Para isso definimos uma relação de equivalência em $R \times S$ e, finalmente, as operações que darão a estrutura de anel a $(R \times S)/\sim$.

Sejam R um anel (não necessariamente comutativo) e $S \subseteq R$. Então S é dito *sistema multiplicativamente fechado* se: $1_R \in S$, $0 \notin S$ e, para quaisquer $s_1, s_2 \in S$, temos $s_1 s_2 \in S$.

Exemplo 1.3.1. Seja R um anel e P um ideal de R. Então $S_P = R \backslash P$ é um sistema multiplicativamente fechado se, e somente se, P é um ideal completamente primo de R.

Sejam R um anel comutativo e $S \subseteq R$ um sistema multiplicativamente fechado de R. Definimos em $R \times S$ a seguinte relação:

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0, \text{ para algum } u \in S.$$

Esta relação é claramente simétrica e reflexiva. Para verificarmos que ela é transitiva consideremos $(a, s), (b, t), (d, u)$ tais que $(a, s) \sim (b, t)$ e $(b, t) \sim (d, u)$. Logo existem $v, w \in S$ tais que $(at - bs)v = 0$ e $(bu - dt)w = 0$, ou seja, $atv = bsv$ e $buw = dtw$. Então multiplicando a primeira igualdade por uw e a segunda por sv obtemos $(au)tvw = (bu)svw$ e $(bu)svw = (ds)tvw$, isto é, $(au)tvw = (ds)tvw$, ou seja, $(au - ds)tvw = 0$, com $tvw \in S$. Portanto $(a, s) \sim (d, u)$, e $\sim$ é uma relação de equivalência em $R \times S$.

Notando por R_S o conjunto quociente $(R \times S)/\sim$ e por $\frac{a}{s}$ a classe do elemento $\overline{(a, s)} \in R_S$, definimos as seguintes operações em R_S:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

É de fácil verificação que as operações acima estão bem definidas, ou seja, não dependem da escolha do representante da classe. Também é fácil verificar que $(R_S, +, \cdot)$, como definido acima, é um anel comutativo, com unidade $\frac{1}{1}$ e elemento neutro aditivo $\frac{0}{1}$.

Podemos agora definir o seguinte homomorfismo de anéis, denominado *homomorfismo canônico*, $\varphi : R \to R_S$ dado por $\varphi(a) = \frac{a}{1}$, para todo $a \in R$. Como $Ker\ \varphi = \{a \in R |\ \exists s \in S \text{ com } as = 0\}$, então φ não é injetora em geral. Além disso, é fácil verificar que este homomorfismo tem as seguintes propriedades:

1. $\varphi(s)$ é invertível em R_S, para todo $s \in S$;

2. $\varphi(a) = 0 \Leftrightarrow \exists s \in S$ tal que $as = 0$;

3. Para todo $x \in R_S$, existem $a \in R$ e $s \in S$ tais que $x = \varphi(a)\varphi(s)^{-1}$.

Para verificarmos (1), mostremos que $\overline{(1, s)}$ é inverso de $\varphi(s)$. Assim, $\varphi(s).\overline{(1, s)} = \overline{(s, 1)}.\overline{(1, s)} = \overline{(s.1, 1.s)} = \overline{(1, 1)}$ e, analogamente, $\overline{(1, s)}\varphi(s) = \overline{(1, 1)}$.

(2) $\varphi(a) = 0_{R_S} \Leftrightarrow \overline{(a, 1)} = 0_{R_S} = \overline{(0, 1)} \Leftrightarrow (a.1 - 0.1)s = 0$, para algum $s \in S$, ou seja, $\varphi(a) = 0 \Leftrightarrow as = 0$, para algum $s \in S$.

(3) Seja $x = \overline{(a, s)} \in R_S$ qualquer. Multiplicando x por $\overline{(s, 1)}$ obtemos, $\overline{(a, s)}.\overline{(s, 1)} = \overline{(as, s)} = \overline{(a, 1)}$, ou seja, $x\varphi(s) = \overline{(a, s)}.\overline{(s, 1)} = \overline{(a, 1)} = \varphi(a)$. Assim, $x = \varphi(a)\varphi(s)^{-1}$.

A terceira propriedade é o motivo da nomenclatura que é dada ao anel R_S o qual é chamado de *anel de frações de R em relação a S*. Observe ainda que, se R é um anel comutativo e P um ideal primo de R, então $S_P = R \backslash P$ é um sistema multiplicativamente fechado e, neste caso, notaremos por R_P ao anel de frações de R em relação a S_P. Também, observamos que se $N(R)$ é o conjunto dos divisores de zero de R, então $S = R\backslash N(R)$ é o maior sistema multiplicativamente fechado de R, e o correspondente anel de frações será chamado *anel total de frações de R*. Chamamos atenção de que neste caso, $\varphi : R \to R_S$ é injetora e podemos considerar $R \subseteq R_S$ como anéis.

Finalizamos esta seção apresentando um resultado que mostra o bom comportamento da soma e da intersecção de ideais com relação as frações. Se I é um ideal de R, então denotaremos por IR_S ao ideal do anel de frações R_S gerado por I, ou seja, $IR_S = \{\frac{a}{s} |\ a \in I,\ s \in S\}$.

Proposição 1.3.2. *Sejam R um anel comutativo, $I,\ J$ ideais de R e $S \subseteq R$ um sistema multiplicativamente fechado. Então temos:*

1. $(I + J)R_S = IR_S + JR_S$

2. $(I \cap J)R_S = IR_S \cap JR_S$

Demonstração. (1) Seja $\frac{a+b}{s} \in (I + J)R_S$, claramente temos $\frac{a+b}{s} = \frac{a}{s} + \frac{b}{s}$ pois $\frac{a}{s} + \frac{b}{s} = \frac{as+bs}{s^2} = \frac{(a+b)s}{s^2} = \frac{a+b}{s}$. Logo, $(I + J)R_S \subseteq IR_S + JR_S$.

Seja $x = \frac{a}{s} + \frac{b}{r} \in IR_S + JR_S$. Pela definição da operação de soma temos $x = \frac{ar+bs}{sr} \in (I + J)R_S$. Logo, $(I + J)R_S = IR_S + JR_S$.

(2) Se $\frac{a}{s} = \frac{b}{t} \in IR_S \cap JR_S$, com $a \in I,\ b \in J$ e $s, t \in S$, então existe $u \in S$ tal que $(at - bs)u = 0$, ou seja, $w = atu = bsu \in I \cap J$. Então $\frac{a}{s} = \frac{w}{stu} \in (I \cap J)R_S$ e, consequentemente, $(I \cap J)R_S \supseteq IR_S \cap JR_S$. A outra inclusão é clara. □

1.3.2 O Caso Geral

Agora vamos estudar o caso mais geral, em que R é um anel qualquer. Naturalmente teremos algumas complicações adicionais. Então começamos com as seguintes definições.

Definição 1.3.3. Sejam R um anel e $S \subseteq R$ um sistema multiplicativamente fechado. Dizemos que um anel T é um *anel de frações à direita de R em relação a S*, se existir um homomorfismo de anéis, chamado *homomorfismo canônico*, $\varphi : R \to T$ tal que:

1. $\varphi(s)$ é invertível em T, para todo $s \in S$;
2. $\forall x \in T,\ x = \varphi(a)\varphi(s)^{-1}$, para certos $a \in R$ e $s \in S$;
3. $\varphi(a) = 0$ se, e somente se, $as = 0$, para algum $s \in S$.

Definição 1.3.4. Sejam R um anel e S um sistema multiplicativamente fechado de R. Então S é dito:

1. *permutável à direita* ou *sistema de Ore à direita*, se para quaisquer $a \in R, s \in S$ tivermos $aS \cap sR \neq 0$, ou seja, se existirem $t \in S, b \in R$ tais que $at = sb$;
2. *reversível à direita*, se para todos $a \in R,\ s \in S$ tais que $sa = 0$, existir $t \in S$ tal que $at = 0$;
3. *conjunto de denominadores à direita*, se S é um conjunto de Ore à direita e reversível à direita.

Proposição 1.3.5. *Seja S um sistema multiplicativamente fechado de um anel R. Então existe um anel de frações à direita de R com respeito a S se, e somente se, S é um conjunto de denominadores à direita.*

Demonstração. Suponhamos que exista um tal anel de frações T e sejam $a \in R$ e $s \in S$. Então, pelo item (2) da Definição 1.3.3, existem $b \in R,\ t \in S$ tais que $\varphi(s)^{-1}\varphi(a) = \varphi(b)\varphi(t)^{-1}$. Assim obtemos que $\varphi(a)\varphi(t) = \varphi(s)\varphi(b)$, ou seja, $\varphi(at - sb) = 0$. Então, pelo item (3) da Definição 1.3.3, $(at - sb)u = 0$, para algum $u \in S$, isto é, $atu = sbu$. Como $tu \in S$, então S é um sistema de Ore à direita. Seja $a \in R$ tal que existe $s \in S$ com $sa = 0$, assim

$0 = \varphi(0) = \varphi(sa) = \varphi(s)\varphi(a)$. Como $\varphi(s)$ é invertível em T, logo obtemos $\varphi(a) = 0$, isto é, existe $t \in S$ tal que $at = 0$. Assim S é um conjunto de denominadores à direita.

Reciprocamente, suponhamos que S seja um conjunto de denominadores à direita de R. Precisamos mostrar que existe um anel de frações à direita de R com respeito a S, e para isso definimos a seguinte relação de equivalência em $R \times S$, dada por:

$$(a, s) \sim (b, t) \Leftrightarrow \exists c, d \in R \text{ tais que } ac = bd \text{ e } sc = td \in S.$$

É fácil ver que $\sim$ é simétrica e reflexiva. Vamos mostrar a transitividade de $\sim$. Sejam $(a, s), (b, t), (r, u) \in R \times S$ tais que $(a, s) \sim (b, t)$ e $(b, t) \sim (r, u)$. Então existem $c, c', d, d' \in R$ tais que $ac = bd$, $sc = td \in S$, $bc' = rd'$ e $tc' = ud' \in S$. Como S é um sistema de Ore à direita, então $(tc')S \cap (td)R \neq 0$, ou seja, existem $x \in R$ e $v \in S$ tais que $tc'v = tdx$, isto é, $t(c'v - dx) = 0$. Como S é reversível à direita, segue que existe $v' \in S$ tal que $(c'v - dx)v' = 0$, ou seja, $c'vv' = dxv'$. Assim temos

$$scx = tdx = tc'v \in S,$$

ou seja,

$$s(cxv') = t(c'vv') = u(d'vv') \in S$$

e, consequentemente,

$$a(cxv') = bdxv' = b(c'vv') = r(d'vv'),$$

de onde segue que $(a, s) \sim (r, u)$, e $\sim$ é transitiva.

Definimos agora as operações em $(A \times S)/\sim$ da seguinte maneira:

$$\overline{(a, s)} + \overline{(b, t)} = \overline{(ac + bd, u)}, \text{ onde } u = sc = td \in S;$$

$$\overline{(a,s)} \cdot \overline{(b,t)} = \overline{(ac,tu)}, \text{ onde } sc = tu \text{ e } u \in S.$$

Não é dificil verificar que as operações acima estão bem definidas e $((R \times S)/\sim, +, \cdot)$ é um anel com unidade $\overline{(s,s)}$, para todo $s \in S$, e elemento neutro aditivo $\overline{(0,t)}$, para todo $t \in S$.

Definimos o seguinte homomorfismo de anéis $\varphi : R \to (R \times S)/\sim$ dado por $\varphi(a) = \overline{(a,1)}$. Vamos ver que essa φ satisfaz as condições da definição de anel de frações.

Tomando $s \in S$, temos $\varphi(s) = \overline{(s,1)}$. Como $\overline{(s,1)} \cdot \overline{(1,s)} = \overline{(su,su)} = 1_{(R\times S)/\sim}$, onde $u \in S$. Então a propriedade (1) da definição de anel de frações está provada.

Dado $\overline{(a,s)} \in (R \times S)/\sim$ qualquer, então temos claramente que $\overline{(a,s)} = \varphi(a) \cdot \varphi(s)^{-1}$. Assim a propriedade (2) da definição de anel de frações está provada.

Finalmente observando que $Ker\ \varphi = \{a \in R |\ \varphi(a) = \overline{(a,1)} = \overline{(0,t)}\} = \{a \in R |\ \exists c, d \in R,$ tais que $ac = 0d$ e $1c = td \in S\} = \{a \in R |\ \exists s \in S$ tal que $as = 0\}$. Portanto, a última propriedade da definição de anel de frações está provada. $\square$

Notaremos por $R[S^{-1}]$ ao anel de frações à direita de R com respeito a S. Agora vamos mostrar que, com as notações da proposição anterior, quando o anel $R[S^{-1}]$ existe, ele possui a seguinte propriedade universal.

Proposição 1.3.6. *Com as notações da proposição anterior, suponhamos que $R[S^{-1}]$ exista. Então para todo homomorfismo de anéis $\psi : R \to T$ tal que $\psi(s)$ é invertível em T, para todo $s \in S$, existe um único homomorfismo de anéis $\rho : R[S^{-1}] \to T$ tal que $\rho \circ \varphi = \psi$, onde φ é o homomorfismo canônico da proposição anterior.*

Demonstração. Definimos $\rho : R[S^{-1}] \to T$, por $\rho(\varphi(a)\varphi(s)^{-1}) = \psi(a)\psi(s)^{-1}$.

Para verificar-mos a boa definição de ρ, tomamos $\overline{(a,s)} = \overline{(a',s')} \in R[S^{-1}]$. Então existem $c,\ d \in R$ tais que $ac = a'd$, e $sc = s'd \in S$. Assim, $\psi(a)\psi(c)$ $= \psi(ac) = \psi(a'd) = \psi(a')\psi(d)$, e $\psi(s)\psi(c) = \psi(sc) = \psi(s'd) = \psi(s')\psi(d) \in \mathcal{U}(T)$. Assim, $\psi(a')\psi(d) = \psi(a')\psi(s')^{-1}\psi(s')\psi(d) = \psi(a')\psi(s')^{-1}\psi(s)\psi(c)$. Por outro lado, $\psi(a)\psi(c) = \psi(a)\psi(s)^{-1}\psi(s)\psi(c)$. Como $\psi(sc) \in \mathcal{U}(T)$, logo temos que $\psi(a)\psi(s)^{-1} = \psi(a')\psi(s')^{-1}$. Portanto, $\rho(\overline{(a,s)}) = \rho(\overline{(a',s')})$. Agora vamos verificar que ρ é homomorfismo, $\rho(\varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1}) = \rho(\varphi(ac+bd)\varphi(u)^{-1}) = \psi(ac+bd)\psi(u)^{-1}$, onde $ac = bd$ e $u = sc = td \in S$. Logo,

$$\begin{aligned}
\psi(ac+bd)\psi(u)^{-1} &= \psi(ac)\psi(u)^{-1} + \psi(bd)\psi(u)^{-1} \\
&= \rho(\varphi(ac)\varphi(u)^{-1}) + \rho(\varphi(bd)\varphi(u)^{-1}) \\
&= \rho(\varphi(ac)\varphi(sc)^{-1}) + \rho(\varphi(bd)\varphi(td)^{-1}) \\
&= \rho(\varphi(a)\varphi(s)^{-1}) + \rho(\varphi(b)\varphi(t)^{-1}).
\end{aligned}$$

Analogamente mostra-se que ρ preserva o produto, portanto ρ é um homomorfismo.

Para mostrarmos que $\rho \circ \varphi = \psi$ tomemos $a \in R$, então $(\rho \circ \varphi)(a) = \rho(\varphi(a)) = \rho(\varphi(a)\varphi(1)^{-1}) = \psi(a)\psi(1)^{-1}$, onde a segunda igualdade vale pois $\varphi(a) = \varphi(a.1) = \varphi(a)\varphi(1)$, assim obtendo $\varphi(a)\varphi(1)^{-1} = \varphi(a)$. Logo $\psi(a) = (\rho \circ \varphi)(a)\psi(1) = (\rho \circ \varphi)(a)$, pois $\psi(1) = 1$.

Para mostrarmos a unicidade da ρ, suponhamos que exista um homomorfismo $\tau : R[S^{-1}] \to T$ tal que $\tau \circ \varphi = \psi$. Seja $x = \varphi(a)\varphi(s)^{-1} \in R[S^{-1}]$ qualquer, então $\tau(x) = \tau(\varphi(a)\varphi(s)^{-1}) = \tau(\varphi(a))\tau(\varphi(s)^{-1}) = \psi(a)\tau(\varphi(s)^{-1})$. Como τ é homomorfismo, $1 = \tau(1) = \tau(\varphi(s)\varphi(s)^{-1}) = \tau(\varphi(s))\tau(\varphi(s)^{-1}) = \psi(s)\tau(\varphi(s)^{-1})$. Assim, temos que $\tau(x) = \psi(a)\tau(\varphi(s)^{-1}) = \psi(a)\psi(s)^{-1} = \rho(\varphi(a)\varphi(s)^{-1}) = \rho(x)$. Portanto $\tau = \rho$ e a proposição está provada. $\square$

Corolário 1.3.7. *Sejam ψ e ρ definidas como na proposição anterior. Se ψ satisfaz as condições (2) e (3) da Definição 1.3.3 de anéis de frações, então*

ρ é um isomorfismo.

Demonstração. Seja $x = \varphi(a)\varphi(s)^{-1} \in Ker\ (\rho)$, então $0 = \rho(\varphi(a)\varphi(s)^{-1}) = \psi(a)\psi(s)^{-1}$. Logo $\psi(a) = 0$, pois $\psi(s)^{-1}$ é invertível. Pela propriedade (3) da definição de anel de frações, que vale para ψ, temos que existe $s' \in S$ tal que $as' = 0$. Assim temos, $0 = \varphi(as') = \varphi(a)\varphi(s')$, logo $\varphi(a) = 0$, pois $\varphi(s')$ é invertível. Portanto $x = \overline{(0, s)} = 0_{R[S^{-1}]}$ e ρ é injetora.

Seja $y \in T$ qualquer. Então $y = \psi(a)\psi(s)^{-1}$, para algum $a \in R$ e $s \in S$. Assim, $y = \psi(a)\psi(s)^{-1} = \rho(\varphi(a)\varphi(s)^{-1})$ e ρ é sobrejetora. □

Corolário 1.3.8. *A menos de isomorfismo, o anel de frações à direita de R com respeito a S é único.*

Naturalmente podemos definir o anel de frações à esquerda de R com respeito a um conjunto de denominadores à esquerda S de R, com as adaptações necessárias. Assim, utilizando o que está descrito acima, podemos construir o anel de frações à esquerda de R com respeito a S, que é unicamente determinado a menos de isomorfismo, que notaremos por $[S^{-1}]R$. O resultado a seguir é uma consequência imediata do corolário anterior.

Corolário 1.3.9. *Sejam R um anel e S um conjunto de denominadores à direita e à esquerda de R. Então $R[S^{-1}] \simeq [S^{-1}]R$ como anéis.*

Finalizaremos esta seção introduzindo os módulos de frações.

Definição 1.3.10. Sejam S um conjunto de denominadores à direita de um anel R e M um R-módulo à direita. Definimos o *módulo de frações* de M com respeito a S como sendo o $R[S^{-1}]$-módulo à direita $M[S^{-1}] = M \otimes_R R[S^{-1}]$ com a estrutura dada pela aplicação canônica.

Esta definição é bastante razoável, em vista dos próximos dois resultados.

Proposição 1.3.11. *A aplicação canônica R-linear $\rho_M : M \to M[S^{-1}]$ tem a seguinte propriedade universal: para cada $R[S^{-1}]$-módulo à direita N e cada aplicação R-linear $\alpha : M \to N$ existe uma única aplicação $R[S^{-1}]$-linear $\sigma : M[S^{-1}] \to N$ tal que $\sigma \circ \rho_M = \alpha$.*

Demonstração. O resultado segue a partir dos isomorfismos naturais

$$\begin{aligned} \operatorname{Hom}_{R[S^{-1}]}(M \otimes_R R[S^{-1}], N) &\simeq \operatorname{Hom}_R(M, \operatorname{Hom}_{R[S^{-1}]}(R[S^{-1}], N)) \\ &\simeq \operatorname{Hom}_R(M, N). \end{aligned}$$

□

Proposição 1.3.12. *Sejam R um anel, S um conjunto de denominadores à direita de R e M um R-módulo à direita. Então $M[S^{-1}] \simeq (M \times S)/\sim$, onde $\sim$ é a relação de equivalência definida por $(x, s) \sim (y, t)$ se existirem $c, d \in R$ tais que $xc = yd$ e $sc = td \in S$.*

Demonstração. Esta prova é similar a feita na Proposição 1.3.5, pela verificação de que para $(M \times S)/\sim$ vale a propriedade universal definida na proposição anterior. As operações em $(M \times S)/\sim$ são definidas por:

$$(x, s) + (y, t) = (xc + yd, u), \text{ onde } u = sc = td \in S;$$

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

O resultado a seguir é análogo ao mostrado na página 15, item (2).

Corolário 1.3.13. *O Kernel da aplicação canônica $\rho : M \to M[S^{-1}]$ consiste dos elementos $x \in M$ para os quais existe $s \in S$ tal que $xs = 0$.*

Capítulo 2

Reticulados

Neste capítulo estudamos reticulados, em especial, reticulados distributivos e damos uma caracterização relacionando complementos relativos à reticulados distributivos, que é usada para fazermos, mais adiante, uma caracterização de anéis e módulos distributivos.

2.1 Reticulados

Começamos definindo o que é um reticulado. Depois, discutiremos algumas de suas propriedades que vão interessar neste trabalho.

Definição 2.1.1. Um reticulado é um sistema $(\mathcal{L}, \leq, \wedge, \vee)$, onde $\mathcal{L}$ é um conjunto, $\leq$ é uma relação de ordem em $\mathcal{L}$ e $\wedge, \vee$ são duas operações binárias definidas em $\mathcal{L}$, satisfazendo as seguintes condições:

1. $x \leq (y \wedge z) \;\Leftrightarrow x \leq y$ e $x \leq z$;
2. $(y \vee z) \leq x \;\Leftrightarrow y \leq x$ e $z \leq x$.

Onde $x \wedge y$ é denominado o *ínfimo* entre x e y, e $x \vee y$ é denominado o *supremo* entre x e y.

Observemos que em um reticulado $\mathcal{L}$, se $x \leq y$ então $x \wedge y = x$ e $x \vee y = y$, e as operações $\wedge, \vee$ são idempotentes, associativas e comutativas.

Exemplos 2.1.2. A seguir apresentaremos alguns exemplos de reticulados, sendo que os dois últimos terão mais destaque neste trabalho.

1. Seja A um conjunto qualquer e tomamos $\mathcal{L} = \mathcal{P}(A)$ o conjunto das partes de A, com a relação de ordem dada pela inclusão de conjuntos. Então $(\mathcal{L}, \subseteq, \cap, \cup)$ é um reticulado.

2. Seja R um anel e M um R-módulo. Tomando $\mathcal{L}$ a família dos submódulos de M, se tem que $(\mathcal{L}, \subseteq, \cap, +)$ é um reticulado.

3. Sejam R um anel e $\mathcal{L}$ a família dos ideais à direita de R. Então temos que $(\mathcal{L}, \subseteq, \cap, +)$ é um reticulado.

Este último exemplo é um caso particular do segundo, considerando R como módulo à direita sobre si próprio, sendo que os submódulos de R_R são exatamente os ideais à direita de R. Analogamente, podemos considerar o reticulado dos ideais à esquerda ou dos ideais bilaterais, de R.

Daqui para frente, estudaremos o reticulado de submódulos e o reticulado de ideais. Iniciaremos observando uma propriedade que esses dois reticulados satisfazem, chamada modularidade.

Definição 2.1.3. Um reticulado $(\mathcal{L}, \leq, \wedge, \vee)$ é dito *modular* se, para todos $x, y, z \in \mathcal{L}$, com $x \leq y$, temos:

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

Observemos que se $x, y, z \in \mathcal{L}$ são tais que $x \leq y$, como $(z \wedge y) \leq z$ e $(z \wedge y) \leq y$, segue que $(z \wedge y) \vee x \leq z \vee x$ e $(z \wedge y) \vee x \leq y \vee x = y$ (pois $x \leq y$). Portanto $(z \wedge y) \vee x \leq (z \vee x) \wedge y$. Logo, para provar que um reticulado $\mathcal{L}$ é modular, basta verificar que $(z \vee x) \wedge y \leq (z \wedge y) \vee x$.

Exemplo 2.1.4. O reticulado $\mathcal{L}_R(M)$, de um R-módulo à direita M, é modular.

Sejam M um R-módulo, K, L, N submódulos de M, com $L \subseteq N$, e seja $x \in (K + L) \cap N$. Então $x = x_1 + x_2$, com $x_1 \in K$ e $x_2 \in L \subseteq N$. Como $x, x_2 \in N$ então $x_1 = x - x_2 \in N$, portanto $x = x_1 + x_2 \in (K \cap N) + L$ e então $(K + L) \cap N \subseteq (K \cap N) + L$. Como a outra contenção sempre vale, então o reticulado de submódulos de M é modular.

Agora vamos provar um resultado sobre reticulados modulares, que será útil mais adiante.

Lema 2.1.5. *Seja $(\mathcal{L}, \leq, \wedge, \vee)$ um reticulado. Se, para quaisquer $x, y, z \in \mathcal{L}$, valer $(x \wedge y) \vee (y \wedge z) \vee (x \wedge z) = (x \vee y) \wedge (y \vee z) \wedge (x \vee z)$, então $\mathcal{L}$ é modular.*

Demonstração. Sejam $x, y, z \in \mathcal{L}$ tais que $z \leq x$, então $(x \wedge y) \vee [(y \wedge z) \vee (x \wedge z)] = (x \wedge y) \vee [(y \wedge z) \vee z] = (x \wedge y) \vee z$, e também $(x \vee y) \wedge [(y \vee z) \wedge (x \vee z)] = (x \vee y) \wedge [(y \vee z) \wedge x] = (y \vee z) \wedge x$, pois $(y \vee z) \wedge x \leq (x \vee y)$. Portanto $(x \wedge y) \vee z = (y \vee z) \wedge x$, e $\mathcal{L}$ é modular. □

2.2 Reticulados Distributivos

O interesse deste trabalho é estudar certos reticulados distributivos, mais precisamente, os anéis e módulos cujo reticulado de ideais e submódulos são distributivos. Para este propósito, estudaremos algumas propriedades gerais dos reticulados distributivos.

Definição 2.2.1. Um reticulado $(\mathcal{L}, \leq, \wedge, \vee)$ é dito *distributivo* se para todos $x, y, z \in \mathcal{L}$ vale:

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

Observemos que dados $x, y, z \in \mathcal{L}$, temos $x \wedge y \leq x$ e $x \wedge z \leq x$, logo $(x \wedge y) \vee (x \wedge z) \leq x$ e também temos $x \wedge y \leq y$ e $x \wedge z \leq z$, logo $(x \wedge y) \vee (x \wedge z) \leq y \vee z$, portanto obtemos que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. Portanto, para provar que um reticulado $\mathcal{L}$ é distributivo, basta mostrar que $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$.

Exemplo 2.2.2. Dado um conjunto A qualquer, é fácil verificar que o reticulado $(\mathcal{P}(A), \subseteq, \cap, \cup)$ é um reticulado distributivo.

A proposição a seguir nos fornece condições equivalentes à distributividade.

Proposição 2.2.3. *Seja* $(\mathcal{L}, \leq, \wedge, \vee)$ *um reticulado. Então as seguintes condições são equivalentes, para todos* $x, y, z \in \mathcal{L}$*:*

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$*;*
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$*;*
3. $(x \wedge y) \vee (y \wedge z) \vee (x \wedge z) = (x \vee y) \wedge (y \vee z) \wedge (x \vee z)$*.*

Demonstração. (1)$\Rightarrow$(2)

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

(2)$\Rightarrow$(3)

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

(3)$\Rightarrow$(1)

Tome $u = (x \wedge y) \vee (y \wedge z) \vee (x \wedge z)$ e $v = (x \vee y) \wedge (y \vee z) \wedge (x \vee z)$, então $x \wedge u = x \wedge v$. Como $x \leq (x \vee y)$ e $x \leq (x \vee z)$ obtemos $x \wedge v = x \wedge (y \vee z)$. Visto que $\mathcal{L}$ é modular, pelo Lema 2.1.5, e que $[(x \wedge y) \vee (x \wedge z)] \leq x$, segue que $x \wedge u = x \wedge \{(y \wedge z) \vee [(x \wedge y) \vee (x \wedge z)]\} = [(x \wedge y) \vee (x \wedge z)] \vee [x \wedge (y \wedge z)]$. Mas como $(x \wedge y \wedge z) \leq (x \wedge y)$ e $(x \wedge y \wedge z) \leq (x \wedge z)$, então obtemos $(x \wedge y) \vee (x \wedge z) = x \wedge u = x \wedge v = x \wedge (y \vee z)$, e portanto $\mathcal{L}$ é distributivo. $\square$

A partir do Lema 2.1.5 e da proposição acima, obtemos imediatamente o seguinte corolário.

Corolário 2.2.4. *Todo reticulado distributivo é modular.*

Adiante veremos um exemplo de um reticulado de submódulos qua não é distributivo, assim nem todo reticulado modular é distributivo, e a recíproca do corolário acima não vale.

Pelo visto anteriormente e pela equivalência (1) $\Leftrightarrow$ (2) da proposição acima, obtemos facilmente que, para um reticulado $(\mathcal{L}, \leq, \wedge, \vee)$ ser distributivo, basta verificar $(x \vee y) \wedge (x \vee z) \leq x \vee (y \wedge z)$.

Agora consideramos um tipo especial de reticulados, os reticulados linearmente ordenados por inclusão.

Definição 2.2.5. Um reticulado $(\mathcal{L}, \leq, \wedge, \vee)$ é dito *linearmente ordenado* se, para quaisquer $a, b \in \mathcal{L}$, temos $a \leq b$ ou $b \leq a$.

Vejamos um exemplo simples de reticulado linearmente ordenado.

Exemplo 2.2.6. Seja o anel $\mathbb{Z}_8$. O reticulado $\mathcal{L}(\mathbb{Z}_8) = \{\langle\bar{0}\rangle, \langle\bar{0}, \bar{4}\rangle, \langle\bar{0}, \bar{2}, \bar{4}, \bar{6}\rangle, \mathbb{Z}_8\}$ é linearmente ordenado por inclusão, pois os ideais de $\mathbb{Z}_8$ são $\langle\bar{0}\rangle$, $\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \langle\bar{6}\rangle$, $\langle\bar{4}\rangle = \{\bar{0}, \bar{4}\}$ e $\mathbb{Z}_8 = \langle\bar{1}\rangle = \langle\bar{3}\rangle = \langle\bar{5}\rangle = \langle\bar{7}\rangle$ e temos $\langle\bar{0}\rangle \subseteq \langle\bar{4}\rangle \subseteq \langle\bar{2}\rangle \subseteq \langle\bar{1}\rangle$. Portanto $(\mathcal{L}(\mathbb{Z}_8), \subseteq, \cap, +)$ é um reticulado linearmente ordenado.

O seguinte corolário será útil adiante.

Corolário 2.2.7. *Seja* $(\mathcal{L}, \leq, \wedge, \vee)$ *um reticulado linearmente ordenado, então* $\mathcal{L}$ *é um reticulado distributivo.*

Demonstração. Sejam $a, b, c \in \mathcal{L}$ quaisquer.

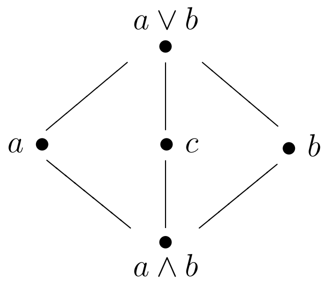
Suponhamos, sem perda de generalidade, que $b \leq c$, então $a \wedge (b \vee c) = a \wedge c \leq (a \wedge b) \vee (a \wedge c)$. Portanto, $\mathcal{L}$ é distributivo. □

Agora queremos mostrar sob quais condições valerá a recíproca do Corolário 2.2.4, e para isso definiremos complementos relativos como segue.

Definição 2.2.8. Sejam $(\mathcal{L}, \leq, \wedge, \vee)$ um reticulado e $a, b \in \mathcal{L}$. Dizemos que um elemento $c \in \mathcal{L}$, tal que $a \wedge b \leq c \leq a \vee b$, é um *complemento de a relativo a b*, se:

1. $a \wedge c = a \wedge b$;
2. $a \vee c = a \vee b$.

Esta definição de complemento relativo pode ser representado sob a forma de diagrama, como mostramos a seguir, onde c é um complemento de a relativo a b.



Vejamos agora um exemplo de complemento relativo.

Sejam K um corpo, V um K-espaço vetorial com $\dim_K V \geq 2$, W um subespaço vetorial de V com $\dim_K W = 2$, e consideremos $u, v, w \in W$ vetores dois-a-dois linearmente independentes. Tomemos V_1 o subespaço vetorial gerado por u, V_2 o subespaço vetorial gerado por v e V_3 o subespaço vetorial gerado por w, então V_3 é um complemento de V_1 relativo a V_2, no reticulado de subespaços vetoriais de V.

O teorema a seguir caracteriza reticulados modulares distributivos através de complementos relativos.

Teorema 2.2.9. *Seja* $(\mathcal{L}, \leq, \wedge, \vee)$ *um reticulado modular. Então* $\mathcal{L}$ *é distributivo se, e somente se, complementos relativos são únicos.*

Demonstração. Suponhamos que $\mathcal{L}$ é um reticulado distributivo e sejam $a, b, c \in \mathcal{L}$, com c complemento de a relativo a b. Então $c = c \wedge (c \vee a) = c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) = (a \wedge b) \vee (c \wedge b) = (a \vee c) \wedge b = (a \vee b) \wedge b = b$. Assim, complementos relativos são únicos.

Reciprocamente, suponha que complementos relativos no reticulado $\mathcal{L}$ sejam únicos. Vamos mostrar que se $\mathcal{L}$ não é distributivo, então conseguimos construir complementos relativos como o diagrama anterior.

Suponhamos, por absurdo, que $\mathcal{L}$ não seja distributivo, então pela Proposição 2.2.3 existem $x, y, z \in \mathcal{L}$ tais que $u = (x \wedge y) \vee (y \wedge z) \vee (x \wedge z) \neq (x \vee y) \wedge (y \vee z) \wedge (x \vee z) = v$. É fácil ver que $u \leq v$.

Consideremos $a = (v \wedge x) \vee u,\ b = (v \wedge y) \vee u$ e $c = (v \wedge z) \vee u$. Assim, $v \wedge x = (x \vee y) \wedge (y \vee z) \wedge (x \vee z) \wedge x = x \wedge (y \vee z)$, de modo análogo, $v \wedge y = y \wedge (x \vee z)$ e $v \wedge z = z \wedge (x \vee y)$. Logo $a \vee b = [x \wedge (y \vee z)] \vee u \vee [y \wedge (x \vee z)] \vee u = [x \wedge (y \vee z)] \vee (x \wedge y) \vee (y \wedge z) \vee (x \wedge z) \vee [y \wedge (x \vee z)] = \{[x \vee (x \wedge y)] \wedge (y \vee z)\} \vee (x \wedge z) \vee \{[y \vee (y \wedge z)] \wedge (x \vee z)\}$, pois $(x \wedge y) \leq y \leq (y \vee z)$, $(y \wedge z) \leq z \leq (x \vee z)$ e $\mathcal{L}$ é modular. Logo $a \vee b = [x \wedge (y \vee z)] \vee (x \wedge z) \vee [y \wedge (x \vee z)] = \{[x \vee (x \wedge z)] \wedge (y \vee z)\} \vee [y \wedge (x \vee z)]$, novamente pois $(x \wedge z) \leq z \leq (y \vee z)$ e $\mathcal{L}$ é modular. Portanto $a \vee b = [x \wedge (y \vee z)] \vee [y \wedge (x \vee z)]$, agora como $x \wedge (y \vee z) \leq x \leq x \vee z$ e novamente usando a modularidade de $\mathcal{L}$, obtemos que $a \vee b = (x \vee z) \wedge \{y \vee [x \wedge (y \vee z)]\} = (x \vee z) \wedge [(y \vee z) \wedge (x \vee y)] = v$, pois $y \leq (y \vee z)$. Analogamente se mostra que $a \vee c = v = a \vee b$.

Agora, como $\mathcal{L}$ é reticulado modular e $u \leq v$, então $a = (x \vee u) \wedge v,\ b = (y \vee u) \wedge v$ e $c = (z \vee u) \wedge v$, e por cálculo análogo ao anterior obtemos que

$a \wedge c = u = a \wedge b$, e portanto c e b são complementos de a relativos a b. Como $b \neq c$, temos uma contradição. Logo $\mathcal{L}$ é distributivo. $\square$

Como consequência do teorema e do exemplo anterior, temos o seguinte:

Exemplo 2.2.10. Sejam K um corpo, V um K-espaço vetorial com $\dim_K V \geq 2$ e $\mathcal{L}_K(V)$ o reticulado dos subespaços vetoriais de V. Então $\mathcal{L}_K(V)$ não é distributivo, pois já vimos que complementos relativos não são únicos neste tipo de reticulado. Assim, espaços vetoriais são exemplos típicos de reticulados modulares que não são distributivos.

Capítulo 3

Anéis e Módulos Distributivos

Neste capítulo estudaremos módulos e anéis distributivos, começaremos fazendo uma tradução do significado do último teorema de caracterização de reticulados distributivos para o contexto de módulos e anéis. Após, discutiremos propriedades básicas destes anéis e módulos, apresentando algumas caracterizações e teoremas de estrutura.

3.1 Definições Iniciais

Definição 3.1.1. Dado um R-módulo M à direita, dizemos que M é um *módulo distributivo* se o reticulado de R-submódulos de M, é distributivo, isto é, se para todos submódulos I, J, K de M tivermos

$$I \cap (J + K) = (I \cap J) + (I \cap K)$$

De maneira análoga, dizemos que um anel R é distributivo à direita (resp. à esquerda) se o reticulado de ideais à direita (resp. à esquerda) é distributivo. E, dizemos que R é distributivo se for distributivo à direita e à esquerda.

Exemplo 3.1.2. O anel $\mathbb{Z}$ dos números inteiros é distributivo.

Como $\mathbb{Z}$ é um domínio de ideais principais, então todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$, para algum $n \in \mathbb{Z}$. Assim, dados dois ideais I, J de $\mathbb{Z}$, existem inteiros a, b tais que $I = a\mathbb{Z}$ e $J = b\mathbb{Z}$. Sabemos que $I + J = mdc(a, b)\mathbb{Z}$ e $I \cap J = mmc(a, b)\mathbb{Z}$. Então, seja $K = c\mathbb{Z}$ um complemento de I relativo a J, isto é, $mdc(a, b)\mathbb{Z} = mdc(a, c)\mathbb{Z}$ e $mmc(a, b)\mathbb{Z} = mmc(a, c)\mathbb{Z}$. Assim, pela fatoração única em primos positivos de um número inteiro, é fácil ver que obrigatoriamente $c = b$. Portanto $\mathbb{Z}$ é distributivo, pelos Teorema 2.2.9 e Exemplo 2.1.4.

A seguir traduziremos a última caracterização de reticulados distributivos para o contexto de módulos e anéis. O resultado a seguir e seus corolários são devidos a Stephenson [12] e [11].

Proposição 3.1.3. *Sejam M um R-módulo qualquer e A, B submódulos de M. Então existe uma correspondência biunívoca entre $Hom(A/(A \cap B), B/(A \cap B))$ e o conjunto dos complementos de B relativos a A no reticulado de R-submódulos de M.*

Demonstração. Podemos supor, sem perda de generalidade, que $A \cap B = 0$, deste modo $A + B = A \oplus B$. Consideremos a aplicação

$$\begin{aligned} \varphi : Hom(A, B) &\to \{X \in \mathcal{L}_R(M) |\ X \oplus B = A \oplus B\} \\ \alpha &\mapsto Ker(\alpha^\star) \end{aligned}$$

onde $\alpha^\star : A \oplus B \to B$ é tal que $\alpha^\star|_A = \alpha$ e $\alpha^\star|_B = I_B$. A aplicação φ está bem definida, pois se existir algum $\gamma : A \oplus B \to B$ com $\gamma|_A = \alpha$ e $\gamma|_B = I_B$, então, para qualquer $a + b \in A \oplus B$, $\gamma(a + b) = \alpha(a) + b = \alpha^\star(a + b)$ e, portanto, $\gamma = \alpha^\star$. Queremos provar que φ é bijetiva.

Sejam $\alpha, \beta \in Hom(A, B)$ tais que $\varphi(\alpha) = \varphi(\beta)$. Dado $a \in A$, $\alpha(a) \in B$, logo $\alpha^\star(\alpha(a)) = \alpha(a) \overset{def}{=} \alpha^\star(a)$, deste modo $(a - \alpha(a)) \in Ker(\alpha^\star) = \varphi(\alpha) = \varphi(\beta) = Ker(\beta^\star)$. Portanto, $0 = \beta^\star(a - \alpha(a)) = \beta^\star(a) - \beta^\star(\alpha(a)) \overset{def}{=} \beta(a) - \alpha(a)$, ou seja, $\beta(a) = \alpha(a)$, e portanto φ é injetiva.

Seja $X \in \mathcal{L}_R(M)$ tal que $X \oplus B = A \oplus B$. Consideremos $p : X \oplus B \to B$ a projeção natural e tomemos $\alpha = p|_A$. Assim temos $\alpha \in Hom(A, B)$ e $\alpha^\star = p$, pois $\alpha^\star|_A = p|_A = \alpha$ e $\alpha^\star|_B = p|_B = I_B$. Portanto $\varphi(\alpha) = X$ e φ é sobrejetiva. $\square$

Corolário 3.1.4. *Seja M um R-módulo à direita. Então M é distributivo se, e somente se, $Hom_R\left(\frac{A}{A\cap B}, \frac{B}{A\cap B}\right) = 0$, para todos $A, B \in \mathcal{L}_R(M)$.*

Demonstração. Pelo Teorema 2.2.9, M é distributivo se, e somente se, complementos relativos são únicos e, pela proposição anterior, complementos relativos são únicos se, e somente se, $Hom_R\left(\frac{A}{A\cap B}, \frac{B}{A\cap B}\right) = 0$ para todos $A, B \in \mathcal{L}_R(M)$. $\square$

Corolário 3.1.5. *Sejam M um R-módulo distributivo e L, N R-submódulos de M. Então:*

1. *Se $L + N = M$, então $Hom_R\left(\frac{M}{L}, \frac{M}{N}\right) = 0$;*
2. *Se $L \cap N = 0$, então $Hom_R(L, N) = 0$.*

Demonstração. 1. Pelo Teorema dos Homomorfismos, temos $\frac{L+N}{L} \simeq \frac{N}{L\cap N}$ e $\frac{L+N}{N} \simeq \frac{L}{L\cap N}$ e, pelo corolário anterior, segue que

$$0 = Hom_R\left(\frac{N}{L\cap N}, \frac{L}{L\cap N}\right) = Hom_R\left(\frac{M}{L}, \frac{M}{N}\right);$$

2. É imediato a partir do corolário anterior. $\square$

Definição 3.1.6. Sejam R um anel, M um R-módulo à direita e P um submódulo de M. Dizemos que P é um submódulo totalmente invariante de M se $\alpha(P) \subseteq P$, para todo $\alpha \in End_R(M)$.

Corolário 3.1.7. *Seja M um R-módulo à direita distributivo. Então todo submódulo maximal de M é totalmente invariante. Em particular, todo ideal à direita maximal de um anel distributivo à direita é bilateral.*

Demonstração. Sejam M um R-módulo e P um submódulo maximal de M. Suponhamos, por absurdo, que exista $\alpha \in End_R(M)$ tal que $\alpha(P) \nsubseteq P$. Logo obtemos que $P + \alpha(P) = M$. Vamos mostrar que $\frac{M}{P} \simeq \frac{M}{\alpha^{-1}(P)}$ e obter que $\alpha^{-1}(P)$ é um submódulo maximal de M.

Consideremos o homomorfismo $\psi : M \to \frac{M}{P} = \frac{\alpha(P)+P}{P}$, dado por $\psi(m) = \alpha(m) + P$, para todo $m \in M$. Dado $m + P \in \frac{M}{P}$ existem $n, p \in P$ tais que $m + P = (\alpha(n) + p) + P = \alpha(n) + P$, logo $\psi(n) = \alpha(n) + P = m + P$ e portanto ψ é sobrejetiva.

Claramente temos que $\alpha^{-1}(P) \subseteq Ker(\psi)$. Seja $x \in Ker(\psi)$ então $0 = \psi(x) \overset{def}{=} \alpha(x) + P$, logo $\alpha(x) \in P$ e portanto $x \in \alpha^{-1}(P)$. Então $Ker(\psi) = \alpha^{-1}(P)$. Pelo Teorema dos Homomorfismos, existe um isomorfismo $\bar{\psi} : M/Ker(\psi) \to \psi(M) = M/P$ e, portanto, $\frac{M}{P} \simeq \frac{M}{Ker(\psi)} = \frac{M}{\alpha^{-1}(P)}$.

Observemos agora que, por hipótese, $P \nsubseteq \alpha^{-1}(P)$ e então obtemos que $\alpha^{-1}(P) + P = M$. Assim, pelo Corolário 3.1.5, temos $Hom(\frac{M}{P}, \frac{M}{\alpha^{-1}(P)}) = 0$, o que é uma contradição, pois $0 \neq \bar{\psi} \in Hom(\frac{M}{P}, \frac{M}{\alpha^{-1}(P)})$. Logo P é um submódulo totalmente invariante de M.

Se R é um anel distributivo à direita, P é um ideal à direita maximal de R e $r \in R$, então consideremos $\alpha_r \in End_R(R)$ definido por $\alpha_r(a) = r.a$, para todo $a \in R$. Assim teremos, $\alpha_r(P) \subseteq P$, isto é, $r.P \subseteq P$ e assim P absorve a multiplicação pela esquerda também. $\square$

Como consequência temos que todo ideal à direita maximal de um anel distributivo à direita é um ideal (bilateral) completamente primo, como será mostrado no próximo resultado.

Corolário 3.1.8. *Sejam R um anel distributivo à direita e P um ideal à direita maximal de R. Então P é ideal (bilateral) completamente primo de R.*

Demonstração. Sejam $a, b \in P$, com $a.b \in P$ e suponhamos que $b \notin P$. Então $P + bR = R$ e, portanto, existem $p \in P$, $r \in R$ tais que $p + br = 1$. Logo, multiplicando por a, obtemos que $a = ap + abr \in P$, pois $ab \in P$. Portanto, P é um ideal (bilateral) completamente primo. Isto completa a prova. $\square$

3.2 Localização em Anéis Distributivos

Sejam R um anel distributivo à direita e P um ideal à direita maximal de R (logo, bilateral), então temos que $S_P = R \backslash P$ é um sistema multiplicativamente fechado de R. Agora queremos saber se sempre é possível "fazer localizações" em R e, quando possível, que tipo de anel de frações obtemos. Vamos começar analisando o caso em que o reticulado de ideais é distributivo, o qual inclui os anéis distributivos comutativos. Antes precisamos de algumas definições.

Definição 3.2.1. Um anel R é dito *aritmético* se o seu reticulado de ideais (bilaterais) é distributivo.

Como vimos anteriormente, $\mathbb{Z}$ é um anel aritmético. Os próximos resultados serão úteis para produzirmos exemplos de anéis aritméticos não comutativos.

Lema 3.2.2. *Se todo anel quociente de um anel R é semiprimo, então R é um anel aritmético.*

Demonstração. Sejam I, J, K ideais de R e definimos $M = I \cap (J + K)$. Então, por hipótese, o anel quociente R/M^2 é um anel semiprimo e segue que M^2 é um ideal semiprimo de R. Logo $M = M^2$ (pois como $M^2 \subseteq M^2$ implica $M \subseteq M^2$). Mas então temos, $M \subseteq M^2 = [I \cap (J+K)][I \cap (J+K)] \subseteq I(J + K) = IJ + IK \subseteq (I \cap J) + (I \cap K) \subseteq I \cap (J + K) = M$ e portanto $(I \cap J) + (I \cap K) = I \cap (J + K)$, ou seja, R é anel aritmético. $\square$

Definição 3.2.3. Um anel R é dito um *anel regular (von Neumann Regular)* se para todo $x \in R$, existir $y \in R$ tal que $x = xyx$.

Um anel de divisão é claramente um anel von Neumann Regular.

Proposição 3.2.4. *Se R é um anel regular, então R é um anel aritmético.*

Demonstração. Sejam I um ideal de R e $a \in R$ tal que $aRa \subseteq I$. Como R é um anel regular, existe $b \in R$ tal que $a = aba \in aRa \subseteq I$, e assim todo ideal I de R é semiprimo. Portanto, o anel quociente R/I é semiprimo, para todo ideal I de R. Segue então do Lema 3.2.2 que R é aritmético. $\square$

Sejam R e $\{R_i |\ i \in I\}$ anéis, e $\epsilon : R \to \prod_{\imath \in I} R_i$ um monomorfismo de anéis. Dizemos que R é um *produto subdireto* dos R_i's, se cada $\pi_i \circ \epsilon : R \to R_i$ é um epimorfismo, onde $\pi_i : \prod_{i \in I} R_i \to R_i$ é o homomorfismo canônico.

Como todo produto subdireto de uma família finita de anéis regulares é um anel regular, tomando um produto subdireto finito de anéis de divisão, obtemos um exemplo não trivial de um anel aritmético que não precisa ser comutativo.

Teorema 3.2.5. *Seja R um anel comutativo. Então as seguintes afirmações são equivalentes:*

1. *R é anel aritmético;*

2. *$\forall \wp \in \mathcal{M}ax(R)$, o reticulado de ideais de $R_\wp$ é linearmente ordenado por inclusão.*

Demonstração. (1) $\Rightarrow$ (2)

Suponhamos que R é um anel aritmético, então $R_\wp$ é aritmético, pois soma e intersecção são preservados por localização (Proposição 1.3.2). Se para quaisquer $x, y \in R_\wp$, temos $x \in yR_\wp$ ou $y \in xR_\wp$, então $I \subseteq J$ ou $J \subseteq I$, para todos I, J ideais à direita de $R_\wp$. De fato, suponhamos que existam I, J tais que $I \not\subseteq J$ e $J \not\subseteq I$. Sejam $a \in J \backslash I$ e $b \in I \backslash J$, assim obtemos que $a \notin bR$ e $b \notin aR$, o que é uma contradição. Deste modo, basta mostrar que dado $\wp \in \mathcal{M}ax(R)$ e dados $x, y \in R_\wp$ temos $x \in yR_\wp$ ou $y \in xR_\wp$.

Notemos o ideal $xR_\wp$ por $\langle x \rangle$. Da distributividade de $R_\wp$ obtemos que $\langle x \rangle = \langle x \rangle \cap (\langle y \rangle + \langle x - y \rangle) = (\langle x \rangle \cap \langle y \rangle) + (\langle x \rangle \cap \langle x - y \rangle)$. Assim x pode ser escrito da forma $x = t + (x - y)c$, com $t \in \langle x \rangle \cap \langle y \rangle$ e $c \in R_\wp$ tal que $yc \in \langle x \rangle$. Desta forma, se $c \in \mathcal{U}(R_\wp)$ então $y \in \langle x \rangle$. Se $c \notin \mathcal{U}(R_\wp)$ então $1 - c \in \mathcal{U}(R_\wp)$, pois $R_\wp$ é um anel local, e segue que $x(1 - c) = t - yc \in \langle y \rangle$ e portanto $x \in \langle y \rangle$. Então eles estão linearmente ordenados por inclusão, e logo o reticulado de ideais de $R_\wp$ é linearmente ordenado.

$(2) \Rightarrow (1)$

Suponhamos que o reticulado de ideais de $R_\wp$ é linearmente ordenado por inclusão, $\forall \wp \in \mathcal{M}ax(R)$. É um fato conhecido em álgebra comutativa que $I = \bigcap_{\wp \in \mathcal{M}ax(R)} IR_\wp$ (Segue da Proposição 3.8 [1] passando ao quociente, ou pela argumentação feita no Lema 3.2.25 adiante). Como o reticulado de ideais de $R_\wp$ é linearmente ordenado por inclusão, segue pelo Corolário 2.2.7 que $R_\wp$ é distributivo. Como soma e intersecção são preservados por localização então, para todos ideais I, J eK de R, temos

$$\begin{aligned} I \cap (J + K) = & \left(\cap_{\wp \in \mathcal{M}ax(R)} IR_\wp\right) \cap \left[\left(\cap_{\wp \in \mathcal{M}ax(R)} JR_\wp\right) + \left(\cap_{\wp \in \mathcal{M}ax(R)} KR_\wp\right)\right] \\ = & [(\cap_{\wp \in \mathcal{M}ax(R)} IR_\wp) \cap (\cap_{\wp \in \mathcal{M}ax(R)} JR_\wp)] + [(\cap_{\wp \in \mathcal{M}ax(R)} IR_\wp) \cap \\ & (\cap_{\wp \in \mathcal{M}ax(R)} KR_\wp)] = (I \cap J) + (I \cap K) \end{aligned}$$

Portanto R é aritmético. $\square$

No Teorema acima provamos basicamente que um anel comutativo aritmético é local se, e somente se, seu reticulado de ideais é linearmente ordenado por inclusão. Assim, obtemos o seguinte resultado.

Corolário 3.2.6. *Seja R um anel comutativo. Então R é aritmético se, e somente se, o reticulado de ideais de R_P é linearmente ordenado por inclusão, para todo ideal primo P de R.*

Lembremos agora, que os ideais primos de $R_\wp$, onde $\wp \in \mathcal{M}ax(R)$, estão em correspondência biunívoca com os ideais primos de R que estão contidos em $\wp$. Portanto os ideais primos de R, que estão contidos em algum ideal maximal, estão linearmente ordenado por inclusão, quando R é aritmético.

Assim obtemos o seguinte resultado.

Corolário 3.2.7. *Seja R um anel comutativo. Se R é anel aritmético e P, Q são ideais primos de R, então temos $P \subseteq Q$ ou $Q \subseteq P$ ou $P + Q = R$.*

Demonstração. Pelo observado acima, se dois ideais primos P e Q de R estão contidos no mesmo ideal maximal, então eles estão linearmente ordenados por inclusão. Em caso contrário, teremos $P \subseteq \wp_1,\ Q \subseteq \wp_2$, onde $\wp_1, \wp_2 \in \mathcal{M}ax(R)$ com $\wp_1 \neq \wp_2$, de modo que $\wp_1, \wp_2 \subset P + Q$, portanto obtemos que $P + Q = R$. $\square$

Agora apresentaremos algumas propriedades que caracterizam a distributividade em anéis e módulos, e algumas de suas consequências. Começamos relembrando algumas propriedade dos R-módulos, que podem ser demonstradas sem muitas dificuldades.

Sejam R um anel, M, N dois R-módulos à direita e $f : M \to N$ um homomorfismo de R-módulos. Então:

1. $f^{-1}f(L) = L + Ker\ f$, para todo R-submódulo L de M;

2. $ff^{-1}(K) = K \cap \mathcal{I}m\ f$, para todo R-módulo K de N;

3. $f(I + J) = f(I) + f(J)$, para todos R-submódulos I, J de M;

4. $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$, para todos R-submódulos P, Q de N.

Em geral não temos a seguinte igualdade, $f(I \cap J) = f(I) \cap f(J)$, onde I, J são R-submódulos de M. O exemplo a seguir mostra isso.

Exemplo 3.2.8. Seja $M = \{x + y\sqrt{2} |\ x, y \in \mathbb{Z}\}$. Então M é um $\mathbb{Z}$-módulo com a adição usual e a multiplicação por inteiros. Consideremos $f : M \to \mathbb{Z}$ definida por $f(x + y\sqrt{2}) = x$. Então f é um homomorfismo que não cumpre a igualdade acima. De fato, tomando $I = \mathbb{Z}$ e $J = \{x + x\sqrt{2} |\ x \in \mathbb{Z}\}$, temos que I, J são dois $\mathbb{Z}$-submódulos de M com $I \cap J = 0$. Mas por outro lado, $f(I) \cap f(J) = \mathbb{Z}$. Assim, $f(I \cap J) = 0 \neq \mathbb{Z} = f(I) \cap f(J)$.

O próximo resultado mostra que essa propriedade realmente caracteriza os módulos distributivos. Este resultado é devido a Stephenson, mas aqui será apresentada uma demonstração feita por Mazurek, por ser mais elementar.

Teorema 3.2.9. *Sejam R um anel e M um R-módulo à direita. As seguintes condições são equivalentes:*

1. *M é distributivo;*
2. *Para todo R-módulo N e todo homomorfismo $f : M \to N$, temos*

$$f(A \cap B) = f(A) \cap f(B), \text{ para todos } R-\text{submódulos de } M;$$

3. *Para todo R-módulo L e todo homomorfismo $g : L \to M$, temos*

$$f^{-1}(A + B) = f^{-1}(A) + f^{-1}(B), \text{ para todos } R-\text{submódulos } A, B \text{ de } M.$$

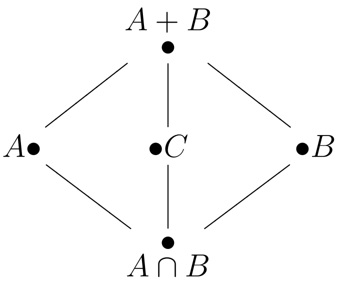
Demonstração. (1) $\Rightarrow$ (2)

Suponhamos que M seja distributivo e consideremos um R-homomorfismo $f : M \to N$, onde N é um R-módulo à direita qualquer. Sejam A, B dois submódulos de M. Então $f^{-1}f(A \cap B) = (A \cap B) + Ker\ f = (A + Ker\ f) \cap (B +$

$Ker\ f) = [f^{-1}f(A)] \cap [f^{-1}f(B)] = f^{-1}[f(A) \cap f(B)]$ e portanto $f(A \cap B) = f(A \cap B) \cap \mathcal{I}m\ f = ff^{-1}[f(A \cap B)] = ff^{-1}[f(A) \cap f(B)] = [f(A) \cap f(B)] \cap \mathcal{I}m\ f = f(A) \cap f(B)$.

$(2) \Rightarrow (1)$

Suponhamos que (2) seja válida e, por absurdo, que M não seja distributivo. Então complementos relativos, no reticulado de submódulos de M, não são únicos, ou seja, podemos encontrar um subreticulado da forma



Considere agora o R-homomorfismo projeção canônica $f : M \to M/C$ dado por $f(a) = a + C$, para todo $a \in M$. Como $A \cap B \subseteq C$, temos $f(A \cap B) = \bar{0}$. Por outro lado, $f(A) = \frac{A+C}{C} = \frac{A+B}{C}$ e $f(B) = \frac{B+C}{C} = \frac{A+B}{C}$, ou seja, $f(A) = \frac{A+B}{C} = f(B)$ e, consequentemente, $f(A \cap B) = \bar{0} \neq \frac{A+B}{C} = f(A) \cap f(B)$, o que é uma contradição.

A equivalência $(1) \Leftrightarrow (3)$ é demonstrada de forma análoga, bastando escolher as propriedades adequadas na primeira implicação e considerar o R-homomorfismo $\imath : C \to M$ no diagrama da segunda implicação. $\square$

Já sabemos, pelo Corolário 2.2.7, que todo reticulado linearmente ordenado é distributivo. Então definiremos os anéis que satisfazem essa propriedade.

Definição 3.2.10. Seja R um anel. Dizemos que R é um *anel de cadeia à direita* (resp. à esquerda) se o reticulado de ideais à direita (resp. à esquerda) for linearmente ordenado por inclusão.

Exemplo 3.2.11. Considere o anel $R = \mathbb{Z}_8$. Conforme já foi mostrado no Exemplo 2.2.6, o reticulado $\mathcal{L}(\mathbb{Z}_8)$ é linearmente ordenado por inclusão, e portanto $\mathbb{Z}_8$ é um anel de cadeia.

Sabemos que um anel R é de cadeia à direita se, e somente se, para todos elementos $a, b \in R$ temos $a \in bR$ ou $b \in aR$. Assim temos uma caracterização de anéis de cadeia, à nível de elementos. O Teorema a seguir nos dá uma caracterização da distributividade, à nível de elementos. Essa caracterização foi obtida por Stephenson [12], mas a primeira implicação será feita seguindo um argumento mais simples devido à Tuganbaev.

Sejam N um R-submódulo de um módulo M qualquer e x um elemento de M. Definimos o *c*ondutor de x em N por: $(N : x) \overset{def}{=} \{r \in R |\ xr \in N\}$, que claramente é um ideal à direita de R.

Teorema 3.2.12. *Sejam R um anel e M um R-módulo à direita. Então M é distributivo se, e somente se, para quaisquer elementos $a, b \in M$ existirem $x, y \in R$ tais que $x + y = 1,\ ax \in bR$ e $by \in aR$.*

Demonstração. Suponhamos M um módulo distributivo à direita e sejam $a, b \in M$. Consideremos $c = a + b$, como $cR = (a + b)R \subseteq aR + bR$ e M é distributivo à direita, temos $cR = cR \cap (aR + bR) = (cR \cap aR) + (cR \cap bR)$. Assim, existem $x, z \in R$ tais que $c = cx + cz$, com $cx \in bR$ e $cz \in aR$. Como $c = a + b$ temos $br \in aR$ se, e somente se, $cr \in aR$ e também $as \in bR$ se, e somente se, $cs \in bR$, isto é, $(aR : c) = (aR : b)$ e $(bR : c) = (bR : a)$. Portanto, $ax \in bR$ e $bz \in aR$. Considerando $w = 1 - (x + z)$, temos que $cw = 0$, logo $w \in (aR : b) \cap (bR : a)$. Agora, consideremos $y = 1 - x = w + z$. Assim teremos $x + y = 1,\ ax \in bR$ e $by = bw + bz \in aR$.

Reciprocamente, suponhamos que o anel satisfaça a condição do Teorema e sejam I, J, K submódulos de M. Queremos provar que $I \cap (J + K) \subseteq (I \cap J) + (I \cap K)$, pois a outra contenção, como já vimos, é sempre válida.

Seja $c = a + b \in I \cap (J + K)$, onde $a \in J$, $b \in K$. Por hipótese, existem $x, y \in R$ com $x + y = 1$, tais que $ax \in bR$ e $by \in aR$. Logo $c = c.1 = c.(x+y) = cx + cy = (a+b)x + (a+b)y \in (cR \cap bR) + (cR \cap aR) \subseteq (I \cap J) + (I \cap K)$, e então $I \cap (J + K) \subseteq (I \cap J) + (I \cap K)$. Portanto M é distributivo. □

Como uma aplicação deste teorema, podemos apresentar o seguinte exemplo.

Exemplo 3.2.13. O reticulado de $\mathbb{Z}$-submódulos de $\mathbb{Q}$ é distributivo.

Dados $x, y \in \mathbb{Q}$, como $\mathbb{Z}$ é comutativo, podemos escrever $x = as^{-1}$ e $y = bs^{-1}$, para certos $a, b, s \in \mathbb{Z}$ e $s \neq 0$. Então temos que $xs = a$ e $ys = b$. Da distributividade de $\mathbb{Z}$ existem $m, n \in \mathbb{Z}$, com $m + n = 1$, tais que $am \in b\mathbb{Z}$ e $bn \in a\mathbb{Z}$, ou seja, $xsm \in ys\mathbb{Z}$ e $ysn \in xs\mathbb{Z}$. E, portanto, existem $\gamma, \lambda \in \mathbb{Z}$ tais que $xsm = ys\gamma$ e $ysn = xs\lambda$, ou seja, $xm = y\gamma \in y\mathbb{Z}$ e $yn = x\lambda \in xR$. Portanto, pelo Teorema acima, $\mathbb{Q}$ é um $\mathbb{Z}$-módulo distributivo.

Veremos agora que alguns resultados válidos para o caso comutativo permanecem válidos em geral. Comecemos com o seguinte resultado para anéis locais.

Proposição 3.2.14. *Sejam R um anel local e M um R-módulo à direita. Se M é distributivo, então o reticulado de R-submódulos de M é totalmente ordenado por inclusão.*

Demonstração. É suficiente provarmos o resultado para os R-módulos principais de M. Suponhamos que M seja distributivo e sejam $x, y \in M$, pelo Teorema 3.2.12, existem $r, s \in R$, com $r + s = 1$, tais que $xr \in yR$ e $ys \in xR$. Logo, se $r \in \mathcal{U}(R)$, temos $x \in yR$, do contrário temos $s = 1 - r \in \mathcal{U}(R)$, pois R é um anel local, e então $y \in xR$. Portanto, os R-submódulos de M são linearmente ordenados por inclusão. □

Suponhamos R um anel distributivo à direita e P um ideal à direita maximal. Então sabemos, pelo Corolário 3.1.8, que P é um ideal (bilateral) completamente primo e, consequentemente, $S_P = R \backslash P$ é um sistema multiplicativamente fechado. O resultado seguinte nos dá mais informações sobre S_P.

Proposição 3.2.15. *Sejam R um anel distributivo e P um ideal à direita maximal de R. Então $S_P = R \backslash P$ é um sistema de Ore à direita.*

Demonstração. Consideremos $a \in R$ e $s \in S_P$. Como R é distributivo à direita, existem $m, n \in R$, com $m + n = 1$, tais que $am \in sR$ e $sn \in aR$. Logo, existem $c, d \in R$ tais que $am = sc$ e $sn = ad$.

Se $n \in P$, então $m = 1 - n \notin P$ e então $aS_P \cap sR \neq$, o que nos diz que S_P é um conjunto de Ore à direita.

Se $n \notin P$, então, como S_P multiplicativamente é fechado, $sn \notin P$ e, consequentemente, $d \notin P$. Portanto novamente temos, $aS_P \cap sR \neq$. □

Definição 3.2.16. Um anel R é dito *l*ocalizável à direita se $S_P = S \backslash P$ for um conjunto de denominadores à direita de R, para todo ideal à direita maximal P de R.

O resultado seguinte é apenas uma síntese dos resultados vistos até agora.

Proposição 3.2.17. *Seja R um anel localizável à direita. Se R é distributivo à direita, então R_P é um anel de cadeia à direita, para todo ideal maximal P de R.*

Demonstração. Suponhamos que R é anel distributivo à direta e sejam $x, y \in R_P$. Então existem $a, b \in R$ e $s \in S_P$ tais que $x = as^{-1}$ e $y = bs^{-1}$. Como R é distributivo existe $z \in R$ tal que $az \in bR$ e $(1 - z)b \in aR$.

Se $z \notin P$, isto é, $z \in S_P$, então z é invertível em R_P e temos $x = as^{-1} = azz^{-1}s^{-1} \in bRz^{-1}s^{-1} \subseteq bR_P = yR_P$. Portanto, $x \in yR_P$.

Se $z \in P$, então $1 - z \in S_P$ e, analogamente, obtemos que $y \in xR_P$. Portanto, R_P é anel de cadeia, para todo ideal maximal P de R. $\square$

Uma questão interessante é saber se a recíproca é verdadeira. Em [2], Brungs provou que a recíproca é verdadeira no caso de R ser anel noetheriano à direita ou domínio. Analisando os argumentos utilizados por Brungs, nota-se que o resultado vale para o caso de R ser um anel localizável à direita. Aqui apresentamos um argumento feito por Tuganbaev.

Proposição 3.2.18. *Seja R um anel localizável à direita. Então R é distributivo à direita se, e somente se, R_P é anel de cadeia à direita, para todo ideal maximal P de R.*

Demonstração. Uma das implicações já foi feita. Suponhamos que R_P seja anel de cadeia à direita, para todo ideal maximal P de R e consideremos $x, y \in R$. Vamos mostrar que $(yR : x) + (xR : y) = R$ e, pelo Teorema 3.2.12, seguirá que R é distributivo.

Por absurdo, suponhamos que exista $P \in \mathcal{M}ax_r(R)$ tal que $(yR : x) + (xR : y) \subseteq P$. Vamos mostrar que existem $a \in R$ e $t \in S_P = S \backslash P$ tais que $xa, y(t - a) \in xR \cap yR$, isto é, $a \in (yR : x)$ e $t - a \in (xR : y)$ e, portanto, $t = a + (t - a) \in (yR : x) + (xR : y) \subseteq P \cap S_P$, o que é uma contradição.

Consideremos $\varphi : R \to R_P$ o homomorfismo canônico. Então R_P se torna um R-módulo à direita via ação: $\forall x \in R_P, r \in R,\ x \cdot r = x\varphi(r)$. Por isso e pelo Corolário 2.2.7, R_P é um R-módulo distributivo à direita, logo existem $q, s_1, s_2 \in R_P$ tais que $\varphi(x)q = \varphi(y)s_1$ e $\varphi(y)(1 - q) = \varphi(x)s_2$. Escrevendo essas frações com o mesmo denominador, podemos assumir que existem $b, c_1, c_2 \in R$ e $u \in S_P$ tais que $q = \varphi(b)\varphi(u)^{-1}$, $s_1 = \varphi(c_1)\varphi(u)^{-1}$

e $s_2 = \varphi(c_2)\varphi(u)^{-1}$. Então, substituindo essas últimas igualdades nas anteriores e multiplicando à esquerda por $\varphi(u)$, obtemos $\varphi(xb) = \varphi(yc_1)$ e $\varphi(y(u-b)) = \varphi(xc_2)$. Portanto existem $v, w \in S_P$ tais que $(xb - yc_1)v = 0$ e $[y(u-b) - xc_2]w = 0$. Então obtemos $xbv, y(u-b)w \in xR \cap yR$.

Como S_P é sistema de Ore, então existem $d, z \in S_P$ tais que $vd = wz$. Logo, tomando $a = bwz \in R$ e $t = uwz \in S_P$, temos que $xa = xbwz = xbvd \in xR \cap yR$ e $y(t-a) = y(uwz - bwz) = y(u-b)wz \in xR \cap yR$. E, pelos argumentos iniciais, a prova está completa. □

Uma outra questão interessante é saber se todos os anéis distributivos à direita são localizáveis à direita. A resposta a essa pergunta foi dada negativamente por Puninsky em [9], através de um exemplo de anel distributivo à direita que não é localizável. Tuganbaev em [14] construiu outro exemplo baseado no exemplo de Puninsky. A seguir damos uma condição suficiente para um anel distributivo ser localizável.

No próximo resultado $N_l(R)$ denota o conjunto dos divisores de zero à esquerda, isto é, $N_l(R) = \{r \in R | \ \exists a \in R \backslash \{0\} \text{ tal que } ar = 0\}$.

Proposição 3.2.19. *Seja R um anel distributivo à direita tal que $N_l(R) \subseteq J(R)$. Então R é um anel localizável à direita.*

Demonstração. Como R é distributivo, sabemos, pela Proposição 3.2.15, que $S_P = R \backslash P$ é sistema de Ore, bastando provar que S_P é reversível à direita, ou seja, se $sa = 0$ com $a \in R$ e $s \in S_P$, então existe $t \in S_P$ tal que $at = 0$.

Suponhamos que $a \in R$ e $s \in S_P$ sejam tais que $sa = 0$. Então $a = 0$, pois do contrário s pertenceria a $N_l(R) \subseteq J(R) \subseteq P$, o que contradiz o fato de $s \in S_P$. Segue então que S_P é um conjunto de denominadores à direita. □

Vejamos o seguinte exemplo de anel distributivo R satisfazendo $N_l(R) \subseteq$

$J(R)$. Consideremos

$$R = \left\{ \begin{pmatrix} a & q \\ 0 & a \end{pmatrix} ; a \in \mathbb{Z},\ q \in \mathbb{Q} \right\}$$

com as operações usuais de soma e multiplicação de matrizes. Neste caso,

$$J(R) = \left\{ \begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix} ; q \in \mathbb{Q} \right\},$$

uma vez que os ideais maximais de R são da forma:

$$M_p = \left\{ \begin{pmatrix} p\mathbb{Z} & \mathbb{Q} \\ 0 & p\mathbb{Z} \end{pmatrix} : p \in \mathbb{Z} \text{ com } p \text{ primo} \right\}.$$

Vamos agora calcular os divisores de zero de R. Sejam $A = \begin{pmatrix} a & q \\ 0 & a \end{pmatrix}$, $B = \begin{pmatrix} b & r \\ 0 & b \end{pmatrix} \in R,\ A \neq 0$, tais que $0_R = A \cdot B = \begin{pmatrix} ab & ar + qb \\ 0 & ab \end{pmatrix}$. Se $a \neq 0$, então $b = 0$ e $r = 0$. Assim, teríamos $B = 0_R$. Se $a = 0$, então $q \neq 0$ e $A \cdot B = \begin{pmatrix} 0 & qb \\ 0 & 0 \end{pmatrix}$. Assim, teríamos $b = 0$ e, portanto, $B = \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$, com $r \in \mathbb{Q}$. Portanto temos, $N_l(R) \subseteq J(R)$ e, pela proposição anterior, R é um anel localizável à direita.

Vamos na direção de uma nova caracterização de distributividade, obtida por M. Ferrero e A. Sant'Ana em [3], que estenderá o resultado de Brungs e que é válida para anéis não localizáveis.

Definição 3.2.20. Sejam R um anel, S um sistema multiplicativamente fechado de R, M um R-módulo à direita e L um R-submódulo de M. Chamamos de *S-saturamento* de L ao conjunto

$$LS^{-1} = \{x \in M |\ \exists s \in S \text{ com } xs \in L\}$$

Diremos que L é *S-saturado* se $LS^{-1} = L$.

Inicialmente LS^{-1} não tem nenhuma estrutura, mas sob certas condições temos que LS^{-1} é um R-submódulo de M.

Proposição 3.2.21. *Sejam R um anel, M um R-módulo à direita, S um sistema de Ore à direita de R e L um R-submódulo de M. Então LS^{-1} é um R-submódulo de M. Além disso, LS^{-1} é S-saturado.*

Demonstração. Claramente, $0 \in LS^{-1}$. Sejam $x, y \in LS^{-1}$, então existem $s, t \in S$ tais que $xs, yt \in L$. Como S é sistema de Ore à direita, então existem $u, v \in S$ tais que $su = tv$. Logo, $(x - y)su = xsu - ysu = xsu - ytv \in L$, portanto $x - y \in LS^{-1}$.

Dado $r \in R$, existem $b \in R$ e $w \in S$ tais que $rw = sb$. Logo, $xrw = xsb \in L$ e, portanto, $xr \in LS^{-1}$.

A última afirmação é imediata do fato de S ser multiplicativamente fechado. $\square$

Observemos que se S é um sistema de Ore à direita de um anel R e $a, b \in R$ são tais que $b \in (aR)S^{-1}$, então existem $r \in R$ e $s \in S$ com $bs = ar$. Dado $u \in (bR)S^{-1}$, temos $ut = bc$, para algum $t \in S$ e $c \in R$. Como S é um sistema de Ore, logo existem $v \in S$ e $d \in R$ tais que $cv = sd$. Assim, $utv = bcv = bsd = ard$. Como $tv \in S$ e $rd \in R$, logo obtemos que $(bR)S^{-1} \subseteq (aR)S^{-1}$. Com este resultado podemos concluir que $(bR)S^{-1}$ é o menor ideal à direita saturado contendo b.

Definição 3.2.22. Dizemos que um anel R é *anel admissível* (à direita) se, para todo ideal à direita maximal P de R, tivermos S_P um sistema de Ore à direita.

Uma consequência da definição acima é, que se R é um anel admissível, então todo ideal à direita maximal P de R é completamente primo, pois S_P

é sistema multiplicativamente fechado. Pelo que estudamos até o momento, sabemos que todo anel distributivo à direita é admissível.

O resultado que segue é uma reescrita do Teorema 3.2.12, pois se $r+s=1$ então não podem ambos pertencer ao mesmo ideal à direita maximal de R.

Proposição 3.2.23. *Sejam R um anel e M um R-módulo à direita. Então M é distributivo se, e somente se, para todos $x, y \in M$ e todo $P \in \mathcal{M}ax_r(R)$, existir $s \in S_P$ tal que $xs \in yR$ ou $ys \in xR$.*

Vamos agora apresentar um resultado de [3], que é o principal resultado desta seção.

Teorema 3.2.24. *Sejam R um anel admissível e M um R-módulo à direita. Então as seguintes afirmações são equivalentes*

1. *M é distributivo;*
2. *O reticulado de R-submódulo S_P-saturados de M é linearmente ordenado por inclusão, para todo $P \in \mathcal{M}ax(R)$;*
3. *O reticulado de R-submódulo S_P-saturados de M é distributivo e fechado para adição.*

Para provar este resultado, vamos precisar de vários lemas auxiliares.

Lema 3.2.25. *Sejam R um anel admissível, M um R-módulo à direita e N um R-submódulo de M. Então*

$$N = \bigcap_{P \in \mathcal{M}ax_r(R)} NS_P^{-1}$$

Demonstração. Claramente temos que $N \subseteq \cap_{P \in \mathcal{M}ax_r(R)} NS_P^{-1}$, para todo $P \in \mathcal{M}ax_r(R)$.

Reciprocamente, seja $x \notin N$. Então $1 \notin (N : x)$, logo existe ideal maximal à direita $\mathcal{P}$ de R tal que $(N : x) \subseteq \mathcal{P}$. Portanto, para todo $s \in S_{\mathcal{P}}$, temos $xs \notin N$ e logo $x \notin NS_{\mathcal{P}}^{-1}$. Portanto, $\cap_{P \in \mathcal{M}ax_r(R)} NS_{\mathcal{P}}^{-1} \subseteq NS_{\mathcal{P}}^{-1} \subseteq N$. $\square$

Lema 3.2.26. *Sejam R um anel admissível e M um R-módulo à direita. Se o reticulado de R-submódulos S_P-saturados de M é fechado para adição, então $(K+N)S_P^{-1} = KS_P^{-1} + NS_P^{-1}$, para todos R-submódulos $K,\ N$ de M.*

Demonstração. Sejam K, N submódulos quaisquer de M, então é claro que $K+N \subseteq (K+N)S_P^{-1} \subseteq (KS_P^{-1} + NS_P^{-1})S_P^{-1}$, pois $K \subseteq KS_P^{-1}$ para todo R-submódulo K de M. Como o reticulado de submódulos S_P-saturados é fechado para soma, então $K+N \subseteq (KS_P^{-1} + NS_P^{-1})S_P^{-1} = KS_P^{-1} + NS_P^{-1}$.

Reciprocamente, seja $a = x + y \in KS_P^{-1} + NS_P^{-1}$, com $x \in KS_P^{-1}$ e $y \in NS_P^{-1}$. Logo existem $s_1, s_2 \in S_P$ tais que $xs_1 \in K$ e $ys_2 \in N$. Como R é admissível, existem $t_1, t_2 \in S_P$ tais que $s_1t_1 = s_2t_2 \in S_P$. Logo temos $as_1t_1 = (x+y)s_1t_1 = xs_1t_1 + ys_1t_1 = xs_1t_1 + ys_2t_2 \in K+N$. Como $s_1t_1 \in S_P$, obtemos que $a \in (K+N)S_P^{-1}$ e segue que $KS_P^{-1} + NS_P^{-1} \subseteq (K+N)S_P^{-1}$. $\square$

Lema 3.2.27. *Sejam R um anel, M um R-módulo à direita e $P \in \mathcal{M}ax_r(R)$ tal que $S_P = R \backslash P$ seja sistema de Ore à direita. Então, para quaisquer R-módulos K, N de M, temos*

$$(K \cap N)S_P^{-1} = KS_P^{-1} \cap NS_P^{-1}.$$

Demonstração. Sejam $P \in \mathcal{M}ax_r(R)$ tal que S_P é sistema de Ore à direita, e K, N R-submódulos de M. Claramente $(K \cap N)S_P^{-1} \subseteq KS_P^{-1} \cap NS_P^{-1}$.

Tomemos $x \in KS_P^{-1} \cap NS_P^{-1}$, então existem $s, t \in S_P$ tais que $xs \in K$ e $xt \in N$. Como S_P é sistema de Ore à direita então existem $u, v \in S_P$ tais que $su = tv \in S_P$. Logo $xsu \in KS_P^{-1}$, mas $xsu = xtv \in NS_P^{-1}$, portanto $x \in (K \cap N)S_P^{-1}$ e $KS_P^{-1} \cap NS_P^{-1} \subseteq (K \cap N)S_P^{-1}$. $\square$

Agora estamos em condições de provar o Teorema 3.2.24.

Demonstração do Teorema 3.2.24. (1) $\Rightarrow$ (2)

Suponhamos R distributivo e sejam $P \in \mathcal{M}ax_r(R)$, K e N dois R-submódulos S_P saturados de M. Assim, $K = KS_P^{-1}$ e $N = NS_P^{-1}$. Suponhamos que $N \nsubseteq K$ e seja $x \in N \backslash K$. Como M é distributivo, segue da Proposição 3.2.23, que para cada $y \in K$ existe $s = s(y) \in S_P$ tal que $xs \in yR \subseteq K$ ou $ys \in xR \subseteq N$, mas a primeira não pode ocorrer, pois se $xs \in K = KS_P^{-1}$ teríamos $x \in K$, o que é uma contradição. Logo $ys \in xR \subseteq N$, para todo $y \in K$, portanto, $y \in NS_P^{-1} = N$ e então $K \subseteq N$.

$(2) \Rightarrow (3)$

Imediato, pois do fato do reticulado de submódulos S_P-saturados de linearmente ordenado por inclusão decorre que este reticulado é distributivo e fechado para adição.

$(3) \Rightarrow (1)$

Sejam K, L, N R-submódulos de M. Então, por aplicação sucessiva dos dois últimos lemas auxiliares, temos $[(K + L) \cap N]S_P^{-1} = (K + L)S_P^{-1} \cap NS_P^{-1} = (KS_P^{-1} + LS_P^{-1}) \cap NS_P^{-1} = (KS_P^{-1} \cap NS_P^{-1}) + (LS_P^{-1} \cap NS_P^{-1}) = (K \cap N)S_P^{-1} + (L \cap N)S_P^{-1} = [(K \cap N) + (L \cap N)]S_P^{-1}$, para todo ideal maximal à direita P de R. Aplicando o primeiro lema auxiliar obtemos que

$$\begin{aligned} (K + L) \cap N = & \bigcap\nolimits_{P \in \mathcal{M}ax_r(R)} [(K + L) \cap N]S_P^{-1} \\ = & \bigcap\nolimits_{P \in \mathcal{M}ax_r(R)} [(K \cap N) + (L \cap N)]S_P^{-1} \\ = & (K \cap N) + (L \cap N). \end{aligned}$$

O Teorema está mostrado. $\square$

Uma consequência do Teorema 3.2.24 é que se M é um R-módulo à direita sobre um anel R qualquer, com a propriedade adicional de que existe $z \in M$ tal que z não é anulado por nenhum elemento não-nulo de R, então a distributividade de M força a distributividade de R. De fato, se existe $z \in M$ com a propriedade acima e M é distributivo, então $R \simeq zR \subseteq M$, logo o reticulado de ideais à direita de R é isomorfo a um subreticulado do reticulado de submódulos de M. Observemos que se $M = R_R$, então a propriedade acima vale, pois nossos anéis possuem unidade. Assim, temos os seguintes corolários.

Corolário 3.2.28. *Sejam R um anel, M um R-módulo à direita contendo um elemento que não é anulado por nenhum elemento não-nulo de R. Então as seguintes afirmações são equivalentes:*

1. *M é distributivo;*
2. *R é distributivo à direita e para todo $P \in \mathcal{M}ax_r(R)$, o reticulado de submódulos S_P-saturados de M é linearmente ordenado por inclusão;*
3. *R é um anel admissível e para todo $P \in \mathcal{M}ax_r(R)$, o reticulado de submódulos S_P-saturados de M é distributivo e fechado para adição.*

Agora, considerando $M = R_R$ temos a seguinte versão dos resultados acima.

Corolário 3.2.29. *As seguintes afirmações são equivalentes:*

1. *R é um anel distributivo à direita;*
2. *Para todos $a, b \in R$ e todo $P \in \mathcal{M}ax_r(R)$, existe $s = s(a, b) \in S_P$ com $as \in bR$ ou $bs \in aR$;*
3. *R é um anel admissível e para todo $P \in \mathcal{M}ax_r(R)$, o reticulado de ideais à direita S_P-saturados de R é linearmente ordenado por inclusão;*
4. *R é um anel admissível e para todo $P \in \mathcal{M}ax_r(R)$, o reticulado de ideais à direita S_P-saturados de R é distributivo e fechado para adição.*

O lema a seguir permite fazermos uma conexão entre os resultados vistos acima e àqueles de distributividade e localização vistos anteriormente. O resultado a seguir foi provado em ([13], Lema 2.2) para domínios distributivos à direita, e provado por Ferrero e Sant'Ana em [3] para o caso geral.

Lema 3.2.30. *Sejam M um R-módulo e $P \in \mathcal{M}ax_r(R)$ tal que exista o anel de frações à direta R_P. Então um submódulo N de M é S_P-saturado se, e somente se, existe um submódulo K de $M_P \overset{not}{=} M[S_P^{-1}]$ tal que $N = h^{-1}(K)$, onde $h : M \to M_P$ é a aplicação canônica.*

Demonstração. Seja N um submódulo S_P-saturado de M. Então, para todo $x \in h^{-1}(NR_P)$ temos $h(x) = h(y)h(s)^{-1}$, para algum $y \in N$ e algum $s \notin P$. Logo, $h(xs - y) = 0$ e $xst - yt = 0$, para algum $t \notin P$. Assim $xst \in N$ e, como N é S_P-saturado, segue que $x \in N$. Portanto $N = h^{-1}(NR_P)$, visto que $h^{-1}(NR_P) \subseteq N$ sempre vale.

Reciprocamente, suponhamos que $N = h^{-1}(K)$ com K um submódulo de M_P, onde $h : M \to M_P$ é a aplicação canônica. Se $x \in M$, $s \notin P$ e $xs \in N$ temos $h(x)h(s) \in K$ e, como $h(s)$ é invertível em R_P, logo obtemos que $h(x) \in K$. Logo $x \in N$ e N é S_P-saturado, como queríamos mostrar. $\square$

Assim, obtemos que se R é um anel localizável à direita então existe uma correspondência biunívoca (preservando inclusões) entre os ideais à direita S_P-saturados de R e o reticulado de ideais à direita de R_P, para todo $P \in \mathcal{M}ax_r(R)$. Portanto, R_P é um anel de cadeia à direita se, e somente se, o reticulado de ideais à direita S_P-saturados é linearmente ordenado por inclusão. Assim, o Corolário 3.2.29 estende o resultado de Brungs, pois vale para anéis distributivos não localizáveis.

Capítulo 4

Grau de Distributividade de um Anel

Estenderemos a noção de distributividade para ω-distributividade, demonstrando um teorema de caracterização e definindo o grau de distributividade de um anel ou módulo. Finalmente, estudaremos o grau de distributividade de certos anéis de matrizes. O material apresentado neste capítulo segue o artigo [3], de Ferrero e Sant'Ana.

4.1 ω-distributividade

Nesta seção estenderemos a noção de distributividade para ω-distributividade e mostraremos alguns resultados importantes. Estudaremos o caso em que ω é um cardinal n finito, obtendo resultados importantes para o cálculo do grau de distributividade do anel de matrizes sobre um anel.

Definição 4.1.1. Sejam ω um cardinal ≥ 2, Ω um conjunto de cardinalidade ω e M um R módulo à direita. Dizemos que M é ω-distributivo se o reticulado de submódulos de M é ω-distributivo, isto é, para qualquer submódulo N e qualquer família de submódulos $(N_i)_{i\in\Omega}$ de M tivermos

$$N + \bigcap_{i\in\Omega} N_i = \bigcap_{i\in\Omega}\left(N + \bigcap_{j\neq i} N_j\right)$$

No que segue, para simplificar notações, se M é um R-módulo e são dados elementos $(x_i)_{i\in\Omega}$ de M, denotaremos por X_i ao submódulo de M gerado pela família $\{x_j |\ j \in \Omega,\ j \neq i\}$.

Seja M um R-módulo. Chamamos de um *subfator* de M, todo submódulo de um quociente de M.

Teorema 4.1.2. *Sejam M um R-módulo e $\omega \geq 2$ um cardinal. Então as seguintes afirmações são equivalentes:*

1. *M é ω-distributivo;*
2. *M não tem subfatores que possam ser decompostos em uma soma direta de ω módulos isomorfos não-nulos;*
3. *Para toda família de elementos $(x_i)_{i\in\Omega}$ de M, temos $\sum_{i\in\Omega}(X_i : x_i) = R$, onde X_i é como acima.*

Demonstração. (1) $\Rightarrow$ (2)

Suponhamos que M seja ω-distributivo. Então é claro que todo subfator S de M é ω-distributivo. Suponhamos que $(K_i)_{i\in\Omega}$ seja uma família independente de submódulos não-nulos de S e que exista um módulo K e isomorfismos $f_i : K_i \to K,\ i \in \Omega$. Sejam $P = \sum_{i\in\Omega} K_i,\ P_j = \sum_{j\neq i} K_i$ e denotaremos por N o submódulo de P, cujos elementos, $\sum_{l=1}^{m} x_{i_l}$, são tais que $\sum_{l=1}^{m} f_{i_l}(x_{i_l}) = 0,\ x_{i_l} \in K_{i_l},\ i_l \in \Omega$. Assim, $\cap_{i\in\Omega} P_i = 0$, $\cap_{i\neq j} P_i = K_j$ e $N + K_j = P$, para todo $j \in \Omega$. E então obtemos que

$$N = N + \cap_{i\in\Omega} P_i = \cap_{j\in\Omega}(N + \cap_{j\neq i} P_j) = \cap_{j\in\Omega}(N + K_j) = P$$

o que é uma contradição.

$(2) \Rightarrow (3)$

Suponhamos, por absurdo, que exista uma família de elementos $(x_i)_{i\in\Omega}$ de M tal que $A = \sum_{i\in\Omega}(X_i : x_i) \neq R$ e consideremos o submódulo $N = \sum_{i\in\Omega} x_iA$ de M, onde X_i é como acima.

Tomando um índice em Ω, digamos 1, e assumindo que $x_1r \in N$. Então existem $x_2, \ldots, x_n \in (x_i)_{i\in\Omega}$ e elementos $a_1, a_2, \ldots, a_n \in A$ tais que $x_1r = x_1a_1 + \cdots + x_na_n$. Assim $x_1(r - a_1) \in X_1$, logo $r - a_1 \in A$ e portanto $r \in A$. Em particular $x_1 \notin N$, pois $A \neq R$, e assim N é um submódulo próprio de M. De maneira análoga, obtemos que $x_ir \in N$ se, e somente se, $r \in A$, para todos $i \in \Omega$.

Denotando por $\varphi_i : x_iR \to M/N$ ao homomorfismo definido por $\varphi_i(x_ir) = x_ir + N$, para todos $r \in R$. Então $Ker(\varphi_i) = x_iA$ e, consequentemente, φ_i induz um monomorfismo $\bar{\varphi}_i : x_iR/x_iA \to M/N$. Portanto, podemos considerar $K_i = x_iR/x_iA$ como um submódulo de M/N.

Assim, pelo visto acima, para $i, j \in \Omega$, a aplicação $f : K_i \to K_j$ definida por $f(x_ir + N) = x_jr + N$ é um isomorfismo de módulos.

Queremos mostrar que $\sum_{i\in\Omega} K_i \subseteq M/N$ é uma soma direta. De fato, suponhamos que $(x_1r_1 + N) + \cdots + (x_nr_n + N) = 0$ em M/N, onde $r_j \in R,\ j \in \Omega,\ j = 1, \ldots, n$. Então existem $a_1, \ldots, a_n, a_{n+1}, \ldots, a_m \in A$ tais que $\sum_{i=1}^{n} x_ir_i = \sum_{j=1}^{m} x_ja_j$, onde $n+1, \ldots, m \in \Omega$. Logo $x_i(r_i - a_i) \in X_i,\ i = 1, \ldots, n$. Assim, $r_i - a_i \in A$ e $r_i \in A, i = 1, \ldots, n$. Consequentemente, $x_ir_i + N = 0$, para $i = 1, \ldots, n$. Então a soma $\sum_{i\in\Omega} K_i$ é direta, o que contradiz a hipótese em (2).

$(3) \Rightarrow (1)$

Suponhamos que N e $(N_i)_{i\in\Omega}$ sejam submódulos de M e tomemos $x \in N + \cap_{j\neq i}N_j$, para todo i. Então para qualquer $i \in \Omega$ existem $x_i \in N$ e $y_i \in \cap_{j\neq i}N_j$ tais que $x = x_i + y_i$. Por hipótese, existem $a_1, \ldots, a_n \in R$, com

$\{1, \ldots, n\} \subseteq \Omega$, tais que $\sum_{i=1}^{n} a_1 = 1$ e $y_i a_i \in \cap_{j \neq i} y_j R$, para todo i. Assim

$$y_i a_i \in \cap_{j \neq i} N_j \cap \sum_{j \neq i} y_j R \subseteq \cap_{l \in \Omega} N_l.$$

Consequentemente, $xa_i = x_i a_i + y_i a_i \in N + \cap_{l \in \Omega} N_l$. Portanto, $x = \sum_{i=l}^{n} xa_i \in N + \cap_{l \in \Omega} N_l$ e concluímos que M é ω-distributivo. $\square$

Agora vejamos algumas consequências interessantes decorrentes do teorema acima.

Um R-módulo M é dito *uniserial* se para quaisquer $x, y \in M$ temos $x \in yR$ ou $y \in xR$. Então podemos comparar elementos em módulos uniseriais. Também, se R é um anel distributivo à direita e P é um ideal completamente primo contido no radical de Jacobson de R, então para todos $a, b \in R$ uma das seguintes condições valem: $a \in bR$, $b \in aR$ ou $(aR)S^{-1} = (bR)S^{-1}$, onde $S = R \backslash P$ é um sistema multiplicativamente fechado de R ([4], Lema 3.3). De fato, como R é distributivo à direita, logo existem $x, y \in R$, com $x + y = 1$, tais que $ax \in bR$ e $by \in aR$. Suponhamos que $a \notin bR$. Então $x = 1 - y \notin \mathcal{U}(R)$, de onde segue que $y \notin J(R)$, ou seja, $y \in S$. Portanto, $b \in (aR)S^{-1}$ e, pelo observado na página 7 (capítulo anterior), obtemos que $(bR)S^{-1} \subseteq (aR)S^{-1}$. Analogamente, se $b \notin aR$, então $(aR)S^{-1} \subseteq (bR)S^{-1}$, e o resultado segue.

No que segue, denotaremos por $S_P = S \backslash P$, onde $P \in \mathcal{M}ax_r(R)$.

O corolário a seguir descreve módulos ω-distributivos em termos de condições de comparabilidade e generaliza a Proposição 3.2.23.

Corolário 4.1.3. *M é ω-distributivo se, e somente se, para toda família $(x_i)_{i \in \Omega}$ de M e para todo $P \in \mathcal{M}ax_r(R)$ existir $i \in \Omega$ e $s \in S_P$ tais que $x_i s \in \sum_{j \neq i} x_j R$.*

Demonstração. Se M é ω-distributivo e $(x_i)_{i \in \Omega}$ é uma família em M temos, pelo Teorema 4.1.2, $\sum_{i \in \Omega} (X_i : x_i) = R$, onde $X_i = \sum_{j \neq i} x_j R$. Então existem

$a_1, \dots, a_n \in R$, $\{1, \dots, n\} \subseteq \Omega$, tais que $\sum_{i=1}^n a_i = 1$ e $x_i a_i \in X_i$, para $i = 1, \dots, n$. Então para algum $i \in \Omega$ devemos ter $a_i \notin P$. Logo $s = a_i \in S_P$ satisfaz as condições desejadas.

Reciprocamente, seja $(x_i)_{i\in\Omega}$ uma família com $\sum_{i\in\Omega}(X_i : x_i) = A$ um ideal à direita próprio de R. Tomando $P \in \mathcal{M}ax_r(R)$ com $A \subseteq P$ e $s \in S_P$ tal que $x_i s \in X_i$, para algum $i \in \Omega$. Assim, $s \in (X_i : x_i) \cap S_P \subseteq A \cap S_P \subseteq P \cap S_P$, o que é uma contradição. Então pelo Teorema 4.1.2 o corolário vale. $\square$

Corolário 4.1.4. *Sejam R um anel admissível e M um R-módulo. Então são equivalentes as seguintes afirmações:*

1. *M é ω-distributivo;*
2. *Para qualquer $(x_i)_{i\in\Omega} \in M$ e qualquer $P \in \mathcal{M}ax_r(R)$, existe i tal que $(x_i R)S_P^{-1} \subseteq (\sum_{j\neq i} x_j R)S_P^{-1}$;*
3. *Para qualquer $(x_i)_{i\in\Omega} \in M$ e qualquer $P \in \mathcal{M}ax_r(R)$, existe i tal que $(\sum_{j\neq i} x_j R)S_P^{-1} = (\sum_{j\in\Omega} x_j R)S_P^{-1}$.*

Demonstração. A equivalência (1) $\Leftrightarrow$ (2) é imediata a partir do Corolário 4.1.3 e da Proposição 3.2.21. A implicação (3) $\Rightarrow$ (2) é clara. Provaremos (2) $\Rightarrow$ (3).

Se $(x_i)_{i\in\Omega}$ é uma família em M e $(x_i R)S_P^{-1} \subseteq (\sum_{j\neq i} x_j R)S_P^{-1}$, então $(\sum_{j\neq i} x_j R)S_P^{-1} \subseteq (\sum_{j\in\Omega} x_j R)S_P^{-1}$. Logo vale (3). $\square$

4.2 n-distributividade

Nesta seção estudaremos o caso em que $\omega = n \geq 2$ é um número cardinal finito. Começaremos com algumas definições.

Definição 4.2.1. Sejam R um anel e M um R-módulo à direita.

1. R é dito um anel de n-cadeia à direita se para quaisquer elementos $r_0, \ldots, r_n$ de R existir i, $0 \leq i \leq n$, tal que r_i está no ideal à direita gerado pelos outros elementos r_j, $j \neq i$.

2. R é dito um anel de Prüfer à direita se R é localizável à direita e para todo $P \in \mathcal{M}ax_r(R)$ o anel de frações R_P é um anel de cadeia à direita.

3. M é dito um módulo n-serial à direita se para quaisquer $x_0, \ldots, x_n$ em M existir i, $0 \leq i \leq n$, tal que $x_i \in \sum_{j \neq i} x_j R$.

É fácil ver que um módulo M é $(n-1)$-serial se, e somente se, para submódulos $N_1, \ldots, N_n$ existir i, $1 \leq i \leq n$, tal que $N_i \subseteq \sum_{j \neq i} N_j$. Também, se M é $(n-1)$-serial segue que para quaisquer $x_1, \ldots, x_n \in M$ temos $\sum_{i=1}^{n}(X_i : x_i) = R$, pois existe $i \in \{1, \ldots, n\}$ tal que $x_i \in \sum_{j \neq i} x_j R$, ou seja, $1 \in (X_i : x_i)$ e, portanto, $1 \in \sum_{i=1}^{n}(X_i : x_i)$. Consequentemente, M é n-distributivo.

Brungs mostrou em ([2], Teorema 1) que, para um anel noetheriano à direita (resp. um domínio), R é um anel de Prüfer à direita se, e somente se, R é um anel distributivo à direita. Como consequência dos resultado já mostrados, vamos fazer a seguinte extensão desse Teorema.

Proposição 4.2.2. *Sejam R um anel localizável à direita e M um R-módulo. Então M é n-distributivo se, e somente se, para qualquer $P \in \mathcal{M}ax_r(R)$ o R_P-módulo M_P é $(n-1)$-serial.*

Demonstração. Por hipótese, para todo $P \in \mathcal{M}ax_r(R)$, $M_P = M \otimes_R R_P$ existe. Denotemos por $h : M \to M_P$ a aplicação canônica. Para $x_1, \ldots, x_n$ em M e $1 \leq i \leq n$, existe $s \in S_P$ tal que $x_i s \in \sum_{j \neq i} x_j R$ se, e somente se, $h(x_i) \in \sum_{j \neq i} h(x_j) R_P$. Então, pelo dito acima e pelo Corolário 4.1.3, o resultado segue facilmente. $\square$

Existe uma outra condição equivalente para M ser um módulo n-distributivo, que é bem conhecida para $n = 2$, conforme vimos em 2.2.3. A prova deste resultado é uma consequência de resultados gerais de reticulados.

Proposição 4.2.3. *M é um módulo n-distributivo se, e somente se, para qualquer submódulo N e qualquer família de submódulos $(N_i)_{i=1}^n$ de M temos*

$$N \bigcap \sum_{i=1}^{n} N_i = \sum_{i=1}^{n} \left(N \bigcap_{j \neq i} N_j \right).$$

Até o final desta seção assumiremos que o anel R tem um único ideal maximal $\mathcal{M}$, ou seja, R é um anel local. Neste caso, $\mathcal{M}$ é igual ao radical de Jacobson $J(R)$ de R e todo elemento $r \in R \backslash \mathcal{M}$ é invertível.

Sabemos que, sob as condições acima, um anel R é dito distributivo (ou seja, 2-distributivo) se, e somente se, R é um anel de cadeia à direita (Proposição 3.2.14). O resultado a seguir é uma extensão desse resultado.

Proposição 4.2.4. *Sejam $(R, \mathcal{M})$ como acima e M um R-módulo. Então M é n-distributivo se, e somente se, M é $(n-1)$-serial.*

Demonstração. Se M é n-distributivo, dados $x_1, \ldots, x_n$ em M, pelo Corolário 4.1.3, existem $i \in \{1, \ldots, n\}$ e $s \notin \mathcal{M}$ tais que $x_i s \in \sum_{j \neq i} x_j R$. Como s é invertível, obtemos que $x_i \in \sum_{j \neq i} x_j R$ e então M é $(n-1)$-serial. A outra implicação já foi observada no início desta seção. $\square$

Se R é um anel comutativo, noetheriano e local, McLean em [8] estudou condições equivalentes para o número de geradores de um ideal ser igual a n. O próximo resultado vai nessa direção e é um pouco mais geral.

Corolário 4.2.5. *Sejam $(R, \mathcal{M})$ como acima e M um R-módulo. Então as seguintes condições são equivalentes:*

1. *M é n-distributivo;*

2. *Qualquer submódulo finitamente gerado de M é gerado por $n-1$ elementos;*

3. *Se $N_1, \ldots, N_n$ são submódulos de M, então existe $i \in \{1, \ldots, n\}$ tal que $N_i \subseteq \sum_{j \neq i} N_j$;*

4. *Para toda família $N_1, \ldots, N_n$ de submódulos de M temos*

$$N \bigcap \sum_{i=1}^{n} N_i = \sum_{i=1}^{n} \left(N \bigcap_{j \neq i} N_j \right).$$

4.3 O Grau de Distributividade de Anéis de Matrizes

Nesta seção vamos definir o grau de distributividade de anéis e módulos, e calcular alguns graus de distributividade, conforme [3], usando o que foi feito até agora. Calcularemos o grau de distributividade de certos anéis de matrizes.

Definição 4.3.1. O *grau de distributividade* de um R-módulo M é o menor cardinal α tal que M é α-distributivo. Analogamente, o *grau de distributividade à direita* de um anel R é o menor cardinal α tal que R_R é α-distributivo.

Sejam K um corpo e V um K-espaço vetorial de dimensão n sobre K. Se tomarmos $v_0, \ldots, v_n \in V$, então existem $k_0, \ldots, k_n \in K$, nem todo nulos, tais que $k_0 v_0 + \cdots + k_n v_n = 0$. Seja i tal que $k_i \neq 0$, logo $v_i = -k_i^{-1} k_0 v_0 - \cdots - k_i^{-1} k_{i-1} v_{i-1} - k_i^{-1} k_{i+1} v_{i+1} - \cdots - k_i^{-1} k_n v_n$. Então V é n-serial. E, pelo visto na seção anterior, V é $(n+1)$-distributivo.

Consideremos agora uma situação mais geral. Sejam R um anel com grau de distributividade à direita $(m+1)$ e L um R-módulo livre de posto n. Em [3] os autores propõem a seguinte questão: *Será que o grau de distributividade de L é $(nm+1)$?* Parece que esta questão não tem, em geral, uma resposta fácil. Em particular, o exemplo a seguir ilustra esta questão.

Um anel R é dito *semissimples* à direita, se R pode ser escrito como soma direta dos seus ideais à direita minimais, isto é, se $R = I_1 \oplus \cdots \oplus I_n$, com $n \in \mathbb{N}$ e $I_1, \ldots, I_n$ ideais à direita minimais de R.

Exemplo 4.3.2. Sejam R um anel semissimples à direita (resp. à esquerda) de grau de distributividade $(m+1)$ e L um R-módulo livre de posto n. Como R é semissimples com grau de distributividade $m+1$, decorre do Teorema 4.1.2(2) que, $R = \bigoplus_{i=1}^{m} S_i$, onde S_i são ideais à direita simples de R. Seja $\{v_1, \ldots, v_n\} \subseteq L$ uma base de L, então $L = \bigoplus_{j=1}^{n} v_j R$, ou seja, $L = \bigoplus_{j=1}^{n} (v_j \bigoplus_{i=1}^{m} S_i)$. Tomando $L_0, \ldots, L_{nm}$ submódulos de L, todos serão escritos como soma dos submódulos simples $v_j S_i$ de L. Desse modo, $\exists k$ tal que $L_k \subseteq \sum_{i \neq k} L_j$. Portanto L é n-serial, e consequentemente L é $(nm+1)$-distributivo.

Em [3], foi conjecturado que o grau de distributividade de um módulo livre de posto n sobre um anel distributivo é $n+1$. Este é o caso quando R é um domínio de cadeia comutativo, como mostra a observação a seguir.

Sejam R um domínio de cadeia comutativo e L um R-módulo livre de posto n. Então L é n-serial.

De fato, tomando $v_0, \ldots, v_n \in L$, temos que $\exists j$ tal que $v_j R \cap \sum_{i \neq j} v_i R \neq 0$. Logo $v_j \alpha_j = \sum_{i \neq j} v_i \alpha_i$. Como R é domínio de cadeia, existe k tal que $\alpha_k \neq 0$ e $\alpha_i = \alpha_k r_{i,k}, \forall i$. Portanto $v_k \alpha_k = \sum_{i \neq k} v_i \alpha_k r_{i,k}$. Assim, $\alpha_k (v_k - \sum_{i \neq k} v_i r_{i,k}) = 0$. Como R é domínio, $\alpha_k \neq 0$ e L é livre, segue que $v_k = \sum_{i \neq k} v_i r_{i,k}$. Deste modo, $v_k \in \sum_{i \neq k} v_i R$. Portanto L é n-serial.

O seguinte exemplo é uma consequência da observação acima e da Proposição 4.2.2.

Exemplo 4.3.3. Sejam R um domínio distributivo comutativo e L um R-módulo à direita de posto n. Então L tem grau de distributividade $n+1$.

Agora queremos calcular o grau de distributividade de um anel de matrizes sobre um anel. Para isso precisaremos de alguns resultados auxiliares.

Lema 4.3.4. *Sejam R um anel e $S = \mathcal{M}_n(R)$ o anel das matrizes $n \times n$ sobre R. Então I é um ideal à direita de S se, e somente se, existe um submódulo N de $\mathbb{R}^n$ tal que I é o conjunto de matrizes cujas colunas são elementos de N.*

Demonstração. É claro que a matriz I cujas colunas pertencem a N é um ideal à direita de S. De fato, pois claramente a matriz nula pertence a I. Dadas duas matrizes de I, $V = (v_1, \dots, v_n)$ e $W = (w_1, \dots, w_n)$, onde $v_1, \dots, v_n, w_1, \dots, w_n$ são as colunas de V e W, respectivamente, que são elementos de N. Então $V - W = (v_1 - w_1, \dots, v_n - w_n) \in I$, pois $(v_i - w_i) \in N$. Dados $B = (b_i)_{1 \leq i \leq n} \in I$, onde $b_i \in N$, e $A = (a_{i,j})_{1 \leq i,j \leq n} \in S$. Então $BA = (a_{1,1}b_1 + \cdots + a_{n,1}b_n, a_{1,2}b_1 + \cdots + a_{n,2}b_n, \dots, a_{1,n}b_1 + \cdots + a_{n,n}b_n)$. Como N é um módulo, as colunas de BA pertencem a N e, portanto, $BA \in I$. Então, o conjunto das matrizes cujas colunas são elementos de N é um ideal à direita de S.

Reciprocamente, seja I um ideal à direita de S e denotamos por N ao conjunto de todos os elementos $v \in R^n$ tais que $(v, 0, \dots, 0) \in I$, onde $(v, 0, \dots, 0)$ é a matriz cuja primeira coluna é v e as demais são nulas. É fácil ver que para qualquer $i \in \{1, \dots, n\}$, N coincide com o conjunto dos $w \in R^n$ tal que existe uma matriz em I cuja i-ésima coluna é w e as demais são zero. De fato, pois multiplicando uma matriz da forma $(v, 0, \dots, 0)$ pela matriz $(a_{l,j})_{1 \leq l,j \leq n}$, onde $a_{1,i} = 1$, com i fixo, e todas as demais entradas são nulas, obtemos a matriz cuja i-ésima coluna é v e as demais são 0. Então dada uma matriz qualquer $A = (a_1, \dots, a_n) \in I$, temos que $a_i \in N$, $i = 1, \dots, n$ e, claramente, N é um submódulo de R^n. $\square$

Corolário 4.3.5. *Para qualquer anel R, o grau de distributividade à direita (resp. à esquerda) do anel $\mathcal{M}_n(R)$ coincide com o grau de distributividade à direita (resp. à esquerda) do módulo à direta (resp. à esquerda) livre R^n.*

Demonstração. É claro, pelo lema anterior, que a aplicação que faz corresponder um submódulo N de R^n ao ideal à direita I de $\mathcal{M}_n(R)$, cujas colunas são elementos de N, define uma bijeção, que preserva intersecções e somas, entre o reticulado de submódulos de R^n e o reticulado dos ideais à direita de $\mathcal{M}_n(R)$. $\square$

Como consequência imediata do exemplo e do corolário acima, obtemos o seguinte exemplo.

Exemplo 4.3.6. Seja R um domínio distributivo e comutativo. Então o grau de distributividade à direita (resp. à esquerda) de $\mathcal{M}_n(R)$ é $n+1$.

Referências Bibliográficas

[1] Atiyah, M., Macdonald, I. *Introduction to Commutative Algebra*. Addilson-Wesley Publishing Company, 1969.

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

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

[4] Ferrero, M., Törner, G. *On the ideal structure of right distributive rings*. Comm. Algebra 21(8) (1993), 2697-2713.

[5] Gratzer, G. *Lattice theory : first concepts and distribuitive lattices*. San Francisco : W.H. Freeman, 1971.

[6] Lam, T. *A first course in noncommutative rings*. Graduate Texts in Mathematics (131), Springer, 1991.

[7] Lam, T. *Lectures on modules and rings*. Graduate texts in mathematics (189), Springer, 1999.

[8] McLean, K. *Local rings with bounded ideals*. J. Algebra 74 (1982), 328-332.

[9] Puninski, G. *Projective modules over the endomorfisms ring of a biuniform module*. J. Pure Appl. Algebra 188 (2004), 227-246.

[10] Stenström, B. *Ring of quotients - introduction to methods of ring theory*. Springer-Verlag, 1975.

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

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

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

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