Universidade Federal de Uberlândia
Faculdade de Matemática

Victor Rodrigues Silva

Decomposição primária de ideais

Uberlândia - MG
2022

Victor Rodrigues Silva

Decomposição primária de ideais

Monografia apresentada à Faculdade de Matemática da Universidade Federal da Uberlândia, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação da Professora Doutora Adriana Rodrigues da Silva.

Uberlândia - MG

2022

Victor Rodrigues Silva

Decomposição primária de ideais

Monografia apresentada à Faculdade de Matemática da Universidade Federal da Uberlândia, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação da Professora Doutora Adriana Rodrigues da Silva.

BANCA EXAMINADORA

Prof. Dra. Adriana Rodrigues da Silva (Orientadora)

Prof. Dr. Victor Gonzalo Lopez Neumann

Profa. Dra. Marisa de Souza Costa

Agradecimentos

À minha mãe, que sempre me apoiou incondicionalmente e fez tudo que estava ao seu alcance para que eu tivesse acesso a melhor educação possível e trilhasse um caminho que ela não teve a oportunidade de trilhar.

Ao meu pai e minha irmã, que acompanharam de perto minha trajetória acadêmica e me incentivaram a persistir nos meus objetivos.

Aos meus amigos e aos colegas de faculdade, que estiveram ao meu lado nos momentos bons e nos ruins, tornando tudo mais fácil.

À minha orientadora Adriana Rodrigues e aos professores Marcus Bronzi e Rosana Jafelice, que contribuíram significamente para minha formação.

Resumo

Neste trabalho desenvolveremos um estudo na área da Álgebra Comutativa, que trata essencialmente dos resultados relacionados aos anéis comutativos com unidade. Os principais tópicos abordados são os ideais, anéis quocientes, módulos, submódulos, anéis de frações e módulos de frações, para então utilizar o conhecimento obtido no decorrer da pesquisa, para realizar um estudo sobre a decomposição primária de ideais. Por fim, após provar dois importantes teoremas que garantem a unicidade de tal decomposição, avançaremos nossos estudos aos anéis Noetherianos, uma vez que nestes anéis também é garantida a existência da decomposição primária.

Palavras-Chave: Álgebra Comutativa, anéis, ideais, módulos, decomposição primária.

Abstract

In this work we will develop a study in the area of Commutative Algebra, which essentially deals with the results related to commutative rings with unity. The main topics covered are ideals, quotient rings, modules, submodules, rings of fractions and modules of fractions, to then use the knowledge obtained in the course of the research, to carry out a study about the primary decomposition of ideals. Finally, after proving two important theorems that guarantee the uniqueness of such decomposition, we will advance our studies to Noetherian rings, since in these rings the existence of the primary decomposition is also guaranteed.

Key-Words: Commutative Algebra, rings, ideals, modules, primary decomposition.

Sumário

Introdução

O estudo da álgebra comutativa, primeiramente conhecida como teoria dos ideais, começou com a obra de Richard Dedekind sobre ideais, baseado nos trabalhos precedentes de Ernst Kummer e Leopold Kronecker. Posteriormente, grandes matemáticos como David Hilbert, Emmy Noether e Emanuel Lasker introduziram algumas outras abordagens para o assunto, que foram essenciais para que a álgebra comutativa se tornasse o que é atualmente.

A decomposição de um ideal em ideais primários é um pilar tradicional da teoria de ideais. Ele fornece a base algébrica para decompor uma variedade algébrica em suas componentes irredutíveis. Nesta monografia, iremos estudar os conceitos e resultados necessários para compreender a existência e a unicidade da decomposição primária de ideais, e como ela fornece uma generalização da fatoração de um inteiro como produto de potências primárias.

No primeiro capítulo, serão abordados conceitos com o intuito de dar uma base e familiarizar o leitor com os resultados fundamentais a respeito dos anéis e ideais, que serão utilizados durante todo o trabalho. Serão apresentadas propriedades, exemplos e resultados sobre homomorfismos de anéis, anéis quocientes, ideais principais, primos, coprimos e maximais, nilradical, radical de Jacobson e operações com ideais.

No segundo capítulo, estenderemos nossos estudos aos módulos, que em geral tem resultados bastantes parecidos com os ideais, uma vez que os ideais são casos particulares de módulos. De posse dos resultados a respeito de A-módulos, submódulos e homomorfismos de módulos, conseguiremos trabalhar com as sequências exatas e o famoso Lema da Serpente.

No terceiro capítulo introduziremos os anéis de frações e módulos de frações, que nos trazem um entendimento sobre o processo de localização, que é uma das ferramentas mais importantes da Álgebra Comutativa. Por fim, no quarto capítulo chegaremos ao objetivo central deste trabalho que é a realização da decomposição primária de ideais e veremos que essa decomposição sempre existe quando se trata de anéis Noetherianos.

Esta monografia se baseia numa leitura do livro "Introduction to Commutative Algebra", dos autores M. F. Atiyah e I. G. MacDonald, referência principal deste trabalho e que se encontra em [1].

Os resultados apresentados nos capítulos 1, 2, 3, 4 e 7 do livro, foram selecionados de forma a construir o caminho necessário para o estudo da decomposição primária de ideais. Todas as demonstrações foram abertas e explicadas com o maior detalhamento possível e exemplos foram adicionados, visando facilitar o entedimento de quem está estudando o assunto pela primeira vez e explicitar a absorção do conteúdo pelo autor deste trabalho.

O livro é bastante denso, e vários resultados não estão provados. As demonstrações destes resultados foram, em geral, feitas pelo autor desta monografia, sendo necessário algumas vezes recorrer a outras fontes. O trabalho de conclusão de curso referenciado em [2] foi utilizado para consultar as provas de alguns resultados sobre anéis e módulos, e o referenciado em [3] foi utilizado para consultar sobre sequências exatas. Dois resultados, devido ao tamanho extenso de suas demonstrações, não foram provados neste trabalho e suas provas podem ser encontrados nas referências [4] e [5], conforme citadas no decorrer do texto.

Capítulo 1

Anéis e Ideais

Iniciaremos nosso estudo com os anéis, o que nos dará uma base para o que será estudado no restante do trabalho. Iremos apresentar os conceitos, propriedades e resultados básicos sobre ideais, principalmente a respeito dos ideais principais, primos e maximais e das operações com ideais.

1.1 Anéis e homomorfismos de anéis

Definição 1.1. *Um anel comutativo com unidade A é um conjunto munido com duas operações internas, chamadas adição e multiplicação, que satisfazem as seguintes condições:*

A1: A adição é associativa, isto é,

$$\forall x, y, z \in A, \quad (x + y) + z = x + (y + z).$$

A2: Existe um elemento neutro com respeito à adição, isto é,

$$\exists 0 \in A, \ tal\ que\ 0 + x = x + 0 = x.$$

A3: Todo elemento de A possui um inverso com respeito à adição, isto é,

$$\forall x \in A, \ \exists\ (-x) \in A, \ tal\ que\ x + (-x) = (-x) + x = 0.$$

A4: A adição é comutativa, isto é,

$$\forall x, y \in A, \quad x + y = y + x.$$

M1: A multiplicação é associativa, isto é

$$\forall x, y, z \in A, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

M2: Existe um elemento neutro com respeito à multiplicação, chamado elemento identidade, isto é,

$$\exists 1 \in A, \text{ tal que } 1 \cdot x = x \cdot 1 = x.$$

M3: A multiplicação é comutativa, isto é,

$$\forall x, y \in A, \quad x \cdot y = y \cdot x.$$

AM: A adição é distributiva com respeito à multiplicação, isto é,

$$\forall x, y, z \in A, \quad x \cdot (y + z) = x \cdot y + x \cdot z \ \ e \ \ (x + y) \cdot z = x \cdot z + y \cdot z.$$

Neste trabalho, usaremos apenas o termo "anel" quando quisermos falar sobre um anel comutativo com unidade.

Definição 1.2. *O anel zero, denotado por* 0*, é o anel trivial, isto é, o anel em que o elemento neutro da adição é igual ao elemento identidade, nesse caso temos que*

$$\forall x \in A, \quad x = x \cdot 1 = x \cdot 0 = 0.$$

Definição 1.3. *Um subconjunto S de um anel A é um subanel de A se S é fechado em relação à adição e multiplicação e se contém o elemento identidade de A.*

Definição 1.4. *Um homomorfismo de anéis é uma aplicação f de um anel A em um anel B tal que:*

i) $f(x + y) = f(x) + f(y)$.

ii) $f(x \cdot y) = f(x) \cdot f(y)$.

iii) $f(1) = 1$.

Em outras palavras, temos que f respeita a adição, multiplicação e elemento identidade. Notemos que da condição $i)$ temos que f é também um homomorfismo de grupos abelianos e que:

a) $f(0) = 0$. De fato, temos que $f(0) = f(0 + 0) = f(0) + f(0)$, logo $f(0)$ é o elemento neutro da adição, e portanto $f(0) = 0$.

b) $f(-x) = -f(x)$. De fato, temos que $0 = f(0) = f(x - x) = f(x) + f(-x)$, logo $f(-x)$ é o inverso aditivo de $f(x)$, e portanto $f(-x) = -f(x)$.

c) $f(x - y) = f(x) - f(y)$. De fato, $f(x - y) = f(x) + f(-y) = f(x) - f(y)$.

Definição 1.5. *Um homomorfismo de anéis bijetor é chamado de isomorfismo. Se existe um isomorfismo entre dois anéis, dizemos que esses anéis são isomorfos.*

Exemplo 1.6. *A aplicação identidade de um subanel S de A no anel A é um homomorfismo de anéis. De fato, dados $x, y \in S$, temos que*

$$f(x+y) = x+y = f(x)+f(y),$$
$$f(x\cdot y) = x\cdot y = f(x)\cdot f(y),$$
$$f(1) = 1.$$

Exemplo 1.7. *Se $f : A \to B$ é um homomorfismo de anéis, então a imagem de f é um subanel de B. De fato, sejam $x, y \in A$, então $f(x), f(y) \in B$ e $f(x)+f(y) = f(x+y)$. Como $x+y \in A$, então $f(x+y) \in Im(f)$. Da mesma forma, $f(x)\cdot f(y) = f(x\cdot y) \in Im(f)$. Como f é homomorfismo de anéis, sabemos que $f(1) = 1$, logo $1 \in Im(f)$. Portanto, $Im(f)$ é um subanel de B.*

Exemplo 1.8. *Se $f : A \to B$ e $g : B \to C$ são homomorfismos de anéis, então a composta $g \circ f : A \to C$ também é. De fato, dados $x, y \in A$,*

$$(g\circ f)(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = (g\circ f)(x) + (g\circ f)(y),$$
$$(g\circ f)(x\cdot y) = g(f(x\cdot y)) = g(f(x)\cdot f(y)) = g(f(x))\cdot g(f(y)) = (g\circ f)(x)\cdot(g\circ f)(y),$$
$$(g\circ f)(1) = g(f(1)) = g(1) = 1.$$

Portanto, $g \circ f$ é um homomorfismo de anéis.

1.2 Ideais e anéis quocientes

Definição 1.9. *Um ideal I de um anel A é um subconjunto de A tal que:*

i) I é um subgrupo aditivo de A, isto é, para todos $x, y \in I$, tem-se que $x - y \in I$.

ii) $AI \subseteq I$, isto é, para todo $x \in A$ e para todo $y \in I$, tem-se que $x\cdot y \in I$.

Exemplo 1.10. *Se $f : A \to B$ é um homomorfismo de anéis, então o núcleo de f é um ideal de A, denotado por $ker(f)$. De fato, temos que $ker(f) \neq \emptyset$, pois $0 \in ker(f)$, uma vez que f é homomorfismo e portanto leva 0 em 0. Agora, sejam $x, y \in ker(f)$. Temos que $f(x-y) = f(x) - f(y) = 0 - 0 = 0$, logo $x - y \in ker(f)$ e então $ker(f)$ é um subgrupo aditivo de A. Agora, seja $z \in A$. Temos que $f(z\cdot x) = f(z)\cdot f(x) = f(z)\cdot 0 = 0$, logo $z\cdot x \in ker(f)$. Portanto, $ker(f)$ é um ideal de A.*

Proposição 1.11. *Se $f : A \to B$ é um homomorfismo de anéis, temos que $ker(f) = 0$ se, e somente se, f é injetor.*

Demonstração. Seja $ker(f) = 0$, se $f(a) = f(b)$, então $f(a) - f(b) = f(a-b) = 0$, logo $b–a \in ker(f)$, e então $b–a = 0$, ou seja, $a = b$ e portanto f é injetora. Por outro lado, seja f injetora e seja $x \in ker(f)$. Então $f(x) = 0$, e como $f(0) = 0$, segue que $f(x) = f(0)$. Como f é injetora, temos $x = 0$. Assim, $ker(f) = 0$. □

Definição 1.12. *Seja I um ideal de um anel A e sejam $x, y \in A$, definimos a relação de equivalência $\sim$ da seguinte maneira: dados $x, y \in A$, temos que $x \sim y$ se, e somente se, $x - y \in I$. A classe de equivalência de um elemento x é o conjunto $\overline{x} = \{x+y : y \in I\} = x+I$. O conjunto $\{\overline{x} = x+I; x \in A\}$ das classes de equivalência formam um anel A/I, chamado de anel quociente, com as operações $+$ e $\cdot$ em A/I definidas como a seguir:*

$$\overline{x} + \overline{y} = (x + I) + (y + I) = (x + y) + I = \overline{x + y} \quad e$$

$$\overline{x} \cdot \overline{y} = (x + I) \cdot (y + I) = (xy) + I = \overline{xy}.$$

Proposição 1.13. *A relação $\sim$ da definição anterior é uma relação da equivalência.*

Demonstração. Sejam $x, y, z \in A$.

i) A relação é reflexiva, isto é, $x \sim x$, pois $x - x = 0 \in I$.

ii) A relação é simétrica, pois se $x \sim y$, então $x - y \in I$, e como I é um ideal, então $-(x - y) \in I$, logo $y - x \in I$.

iii) A relação é transitiva, pois se $x \sim y$ e $y \sim z$, então $x - y \in I$ e $y - z \in I$, e como I é um ideal, então $(x - y) + (y - z) \in I$, logo $x - z \in I$, e então $x \sim z$.

□

Observação 1.14. *O anel quociente A/I é de fato um anel, com $\overline{1} = 1 + I$ e $\overline{0} = 0 + I = I$.*

Exemplo 1.15. *A função $\phi : A \to A/I$, que leva cada $x \in A$ em sua classe de equivalência $x + I$, é um homomorfismo de anéis, chamado projeção canônica de A em A/I. De fato, sejam $x, y \in A$, temos que:*

$$\phi(x + y) = (x + y) + I = (x + I) + (y + I) = \phi(x) + \phi(y),$$
$$\phi(x \cdot y) = (x \cdot y) + I = (x + I) \cdot (y + I) = \phi(x) \cdot \phi(y),$$
$$\phi(1) = 1 + I.$$

Esse homomorfismo é sobrejetor pois para todo $z + I \in A/I$, existe $z \in A$ tal que $\phi(z) = z + I$.

Teorema 1.16 (Teorema Fundamental dos Homomorfismos para Anéis)**.** *Seja $f : A \to B$ um homomorfismo de anéis, então f induz um isomorfismo de anéis $A/ker(f) \simeq Im(f)$.*

Demonstração. Considere a função $\overline{f} : A/ker(f) \to Im(f)$, definida por $\overline{f}(\overline{x}) = f(x)$, e sejam $\overline{x}, \overline{y} \in A/ker(f)$. Então, temos que

$$\overline{x} = \overline{y} \Leftrightarrow \overline{x} - \overline{y} = \overline{0} \Leftrightarrow x - y \in ker(f) \Leftrightarrow f(x-y) = 0 \Leftrightarrow f(x) - f(y) = 0 \Leftrightarrow f(x) = f(y) \Leftrightarrow \overline{f}(\overline{x}) = \overline{f}(\overline{y}).$$

Portanto, a função $\overline{f}$ está bem definida e é injetora.

Agora, seja $z \in Im(f)$, então $z = f(x)$, para algum $x \in A$. Logo, $\overline{f}(\overline{x}) = f(x) = z$. Portanto, $\overline{f}$ é sobrejetora.

Além disso,

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x+y}) = f(x+y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y}),$$
$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(x \cdot y) = f(x) \cdot f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y}) \text{ e}$$
$$\overline{f}(\overline{1}) = f(1) = 1.$$

Logo, $\overline{f}$ é um homomorfismo. Portanto, $A/ker(f)$ é isomorfo a $Im(f)$, como queríamos provar. □

Teorema 1.17. *Sejam I e J ideais de um anel A. Se $I \subseteq J$, então J/I é um ideal de A/I e há um isomorfismo de anéis $(A/I)/(J/I) \simeq (A/J)$.*

Demonstração. Considere o homomorfismo $\phi : A/I \to A/J$, definido por $\phi(a+I) = a + J$. O homomorfismo está bem definido pois, se $a + I = b + I$, então $a - b \in I$, e como $I \subseteq J$, então $a - b \in J$, logo $a + J = b + J$. Temos que ϕ é um homomorfismo, pois dados $a + I, b + I \in A/I$, então

$$\phi((a+b)+I) = ((a+b)+J) = (a+J) + (b+J) = \phi(a+I) + \phi(b+I),$$
$$\phi(ab+I) = ab + J = (a+J)(b+J) = \phi(a+I) \cdot \phi(b+I) \text{ e}$$
$$\phi(1+I) = 1 + J.$$

Além disso, temos que $ker(\phi) = \{a + I \in A/I : \phi(a+I) = 0 + J\} = \{a + I \in A/I : a + J = 0 + J\} = \{a + I \in A/I : a \in J\} = J/I$. Temos também que ϕ é sobrejetor pois para todo $a + J \in A/J$, temos que $a + J = \phi(a + I)$, com $a + I \in A/I$, logo $Im(\phi) = A/J$. Portanto, pelo Teorema 1.16, segue que $(A/I)/ker(\phi) \simeq Im(\phi)$, logo $(A/I)/(J/I) \simeq (A/J)$, como queríamos provar. □

Teorema 1.18 (Teorema da Correspondência entre Ideais)**.** *Seja I um ideal do anel A, então existe uma correspondência biunívoca entre os ideais J de A que contém I e os ideias $\overline{J}$ de A/I, dados por $J = \phi^{-1}(\overline{J})$.*

Demonstração. Sejam X o conjunto dos ideais de A que contém I, Y o conjunto dos ideais de A/I, $J \in X$ e $\overline{J} \in Y$. Definimos as funções $\phi : X \to Y$ por $\phi(J) = J/I$ e $\psi : Y \to X$ por $\psi(\overline{J}) := \{a \in A \ : \ a + I \in \overline{J}\}$. Vamos mostras que essas funções estão bem definidas, isto é, que $\phi(J)$ é um ideal de A/I e que $\psi(\overline{J})$ é um ideal de A contendo I.

- Sejam $x,\ y \in J$, então $x+I,\ y+I \in J/I$. Vamos mostrar que $\phi(J)$ é um ideal de A/I. De fato, $(x + I) + (y + I) = (x + y) + I \in J/I$, pois $x + y \in J$, uma vez que J é ideal de A. Além disso, $-(x + I) = -x + I \in J/I$, pois $-x \in J$, uma vez que J é ideal de A. Por fim, se $a + I \in A/I$, então $(a + I)(x + I) = ax + I \in J/I$, pois $ax \in J$, novamente por J ser ideal de A. Portanto $\phi(J) = J/I$ é um ideal de A/I.

- Sejam $x,\ y \in \psi(\overline{J})$, então $x + I,\ y + I \in \overline{J}$. Vamos mostrar que $\psi(\overline{J})$ é um ideal de A. De fato, $(x + y) + I = (x + I) + (y + I) \in \overline{J}$, pois $x + I,\ y + I \in \overline{J}$ e $\overline{J}$ é ideal de A/I, logo $x + y \in \psi(\overline{J})$. Além disso, $-x + I = -(x + I) \in \overline{J}$, pois $x + I \in \overline{J}$ e $\overline{J}$ é ideal de A/I, logo $-x \in \psi(\overline{J})$. Por fim, se $a \in A$, então $ax + I = (a + I)(x + I) \in \overline{J}$, pois $a + I \in A/I$ e $x + I \in \overline{J}$, novamente por $\overline{J}$ ser ideal de A/I, logo $ax \in \psi(\overline{J})$. Portanto $\psi(\overline{J})$ é um ideal de A. Agora, vamos mostrar que $\psi(\overline{J})$ contém I. De fato, se $x \in I$ então $x + I = I = 0 + I \in \overline{J}$, pois $\overline{J}$ é um ideal de A/I, logo $x \in \psi(\overline{J})$. Portanto, $\psi(\overline{J})$ é um ideal de A contendo I.

Agora, vamos mostrar que para todo $J \in X$ e para todo $\overline{J} \in Y$, temos que $\psi(\phi(J)) = J$ e que $\phi(\psi(\overline{J})) = \overline{J}$.

- Temos que $\psi(\phi(J)) = \psi(J/I) = \{a \in A : a + I \in J/I\}$. Mas $a + I \in J/I$ significa que existe $j \in J$ tal que $a + I = j + I$, isto é, $a - j = i \in I$, assim $a = i + j \in J$ sendo $I \subseteq J$. Por outro lado, é claro que se $a \in J$, então $a + I \in J/I$. Isso mostra que $a + I \in J/I$ é equivalente a $a \in J$, logo $\psi(\phi(J)) = \{a \in A \ : \ a \in J\} = J$. Portanto, para todo $J \in X$, temos que $\psi(\phi(J)) = J$.

- Temos que $\phi(\psi(\overline{J})) = \{a \in A : a + I \in \overline{J}\}/I$. Suponha que $x + I \in \phi(\psi(\overline{J}))$, então $x + I = a + I$, com $a + I \in \overline{J}$, logo $x + I \in \overline{J}$. Portanto, $\phi(\psi(\overline{J})) \subseteq \overline{J}$. Agora, suponha que $t = a + I \in \overline{J}$, então $a \in \psi(\overline{J})$, logo $t = a + I \in \phi(\psi(\overline{J}))$. Portanto, $\overline{J} \subseteq \phi(\psi(\overline{J}))$. Assim, para todo $\overline{J} \in Y$, temos que $\phi(\psi(\overline{J})) = \overline{J}$.

Logo, ϕ e ψ são bijeções inversas uma da outra, como queríamos provar. □

1.3 Divisores de zero, elementos nilpotentes e unidades

Definição 1.19. *Um divisor de zero em um anel A é um elemento $x \in A$, para o qual existe $y \neq 0$ em A, tal que $x \cdot y = 0$.*

Exemplo 1.20. *Os elementos* $\overline{2}$ *e* $\overline{3}$ *são divisores de zero do anel* $\mathbb{Z}_6$*, pois* $\overline{2} \cdot \overline{3} = \overline{0}$ *em* $\mathbb{Z}_6$*.*

Definição 1.21. *Um anel sem divisores de zero não nulos é chamado de domínio de integridade.*

Exemplo 1.22. *O anel* $\mathbb{Z}$ *é um domínio de integridade, pois dados* $a, b \in \mathbb{Z}$*, temos que* $a \cdot b = 0$ *se, e somente se,* $a = 0$ *ou* $b = 0$*.*

Exemplo 1.23. *O anel* $\mathbb{Z}_6$ *não é um domínio de integridade, pois vimos no Exemplo 1.6 que* $\mathbb{Z}_6$ *possui divisores de zero não nulos.*

Definição 1.24. *Seja* $x \in A$*. Dizemos que* x *é um elemento nilpotente se* $x^n = 0$*, para algum* $n > 0$*.*

Exemplo 1.25. *Seja* $A \neq 0$ *um anel, então todo elemento nilpotente* $x \neq 0$ *de* A *é um divisor de zero. De fato, seja* n *o menor inteiro positivo tal que* $x^n = 0$*. Temos que* $n \neq 1$*, pois nesse caso teríamos* $x = 0$*, assim* $n > 1$ *e* $n - 1 > 0$*. Então,* $0 = x^n = x \cdot x^{n-1}$*, com* $x \neq 0$ *e* $x^{n-1} \neq 0$*.*

Por exemplo, $\overline{2}$ *é um elemento nilpotente de* $\mathbb{Z}_8$*, pois* $\overline{2}^3 = \overline{2} \cdot \overline{2} \cdot \overline{2} = \overline{8} = \overline{0}$*, e* $\overline{2}$ *é divisisor de zero de* $\mathbb{Z}_8$*, pois* $\overline{2} \cdot \overline{4} = \overline{8} = \overline{0}$*. A recíproca não é verdadeira, ou seja, nem todo divisor de zero de um anel* A *é um elemento nilpotente de* A*, por exemplo,* $\overline{3}$ *é divisor de zero de* $\mathbb{Z}_6$*, pois* $\overline{3} \cdot \overline{2} = \overline{6} = \overline{0}$*, mas* $\overline{3}$ *não é um elemento nilpotente de* $\mathbb{Z}_6$*, pois* $\overline{3}^n = \overline{3} \neq \overline{0}$*, para todo* $n > 0$*.*

Definição 1.26. *Uma unidade de um anel* A *é um elemento* $x \in A$*, para o qual existe* $y \in A$*, tal que* $x \cdot y = 1$*. O elemento* y *é determinado de forma única por* x *e denotado por* x^{-1}*.*

Exemplo 1.27. *As unidades do anel* $\mathbb{Z}$ *são 1 e -1, pois* $1 \cdot 1 = 1$ *e* $(-1) \cdot (-1) = 1$*.*

Exemplo 1.28. *As unidades de um anel* A *formam um grupo abeliano em relação a multiplicação. De fato, seja* G *o grupo das unidades de* A*, então:*

- $1 \in G$*;*
- *Dados* $x, y \in G$*, temos que* $(x \cdot x^{-1}) \cdot (y \cdot y^{-1}) = 1$*, o que implica* $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = 1$*, logo* $x \cdot y \in G$*;*
- *Dado* $x \in G$*, temos que* $x \cdot x^{-1} = 1$*, logo* $x^{-1} \in G$*.*

Definição 1.29. *Seja* $x \in A$*, então* $Ax = \{a \cdot x : a \in A\}$ *é um ideal de* A*, denotado por* (x) *e chamado de ideal gerado por* x*. Se* $I = (x)$ *para algum* $x \in A$*, então dizemos que* I *é um ideal principal.*

Exemplo 1.30. *Sejam* A *um anel e* $x \in A$*. Então,* x *é uma unidade de* A *se, e somente se,* $(x) = A = (1)$*. De fato, se* x *é uma unidade de* A*, então existe* $x^{-1} \in A$*, tal que* $x \cdot x^{-1} = 1$*, logo* $1 \in (x)$*. Como* (x) *é um ideal que contém* 1*, então* $A \cdot 1 = A \subseteq (x)$ *e, portanto,* $(x) = A$*. Por outro lado, se* $(x) = A$*, então* $1 \in (x)$*, pois* $1 \in A$*. Assim, existe* $y \in A$*, tal que* $x \cdot y = 1$*, concluindo que* x *é uma unidade em* A*.*

Definição 1.31. *Um anel A em que $1 \neq 0$ e que todo elemento não nulo é uma unidade é chamado de corpo.*

Proposição 1.32. *Todo corpo é um domínio de integridade.*

Demonstração. De fato, sejam A um corpo e $x, y \in A$, com $x \neq 0$. Suponha que $x \cdot y = 0$, então $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$, logo $(x^{-1} \cdot x) \cdot y = 0$, o que implica $1 \cdot y = 0$ e então $y = 0$. Portanto, x não é divisor de zero. □

Exemplo 1.33. *A recíproca da Proposição anterior é falsa. Por exemplo, vimos no Exemplo 1.7 que $\mathbb{Z}$ é um domínio de integridade, mas vimos no Exemplo 1.10 que as únicas unidades de $\mathbb{Z}$ são 1 e -1, logo $\mathbb{Z}$ não é um corpo.*

Proposição 1.34. *Seja $A \neq 0$ um anel. Então as seguintes afirmações são equivalentes:*

(i) A é um corpo.

(ii) Os únicos ideais de A são (0) e $(1) = A$.

(iii) Todo homomorfismo de A em um anel $B \neq 0$ é injetor.

Demonstração. *i)* $\Rightarrow$ *ii)* Seja A um corpo e $I \neq 0$ um ideal de A. Então I contém um elemento $x \neq 0 \in A$. Como A é corpo, temos que x é uma unidade de A e portanto, pelo Exemplo 1.12, temos que $(x) = A = (1)$. Sabemos que $I \subseteq (1) = A$, pois I é um ideal de A, e temos que $(1) = (x) \subseteq I$ pela definição de ideal. Logo, $I = (1) = A$.

ii) $\Rightarrow$ *iii)* Seja $\phi : A \to B$ um homomorfismo de anéis. Vimos no Exemplo 1.4 que $ker(\phi)$ é um ideal de A, logo $ker(\phi) = (0)$ ou $ker(\phi) = A$. Mas pela definição de homomorfismo sabemos que $f(1) = 1$, logo $ker(\phi) \neq A$ e então a única possibilidade é que $ker(\phi) = 0$. Portanto ϕ é injetor.

iii) $\Rightarrow$ *i)* Seja $x \in A$ um elemento que não é unidade. Então, pelo Exemplo 1.12 temos que $(x) \neq (1)$, e portanto $B = A/(x)$ é não nulo. Seja $\phi : A \to B$ a projeção canônica, cujo núcleo é (x). Por hipótese, ϕ é injetor, então $(x) = 0$, logo $x = 0$. Como todo elemento que não é uma unidade é nulo, então todo elemento não nulo é uma unidade, portanto A é um corpo. □

1.4 Ideais primos e ideais maximais

Definição 1.35. *Um ideal P de A é chamado de ideal primo de A se $P \neq A$ e se dados $x, y \in A$, sempre que $x \cdot y \in P$, tivermos que $x \in P$ ou $y \in P$.*

Exemplo 1.36. *O ideal $2\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$, pois $2\mathbb{Z} \neq \mathbb{Z}$ e dados $x, y \in \mathbb{Z}$, se $x \cdot y \in 2\mathbb{Z}$, então $x \cdot y = 2n$, para algum $n \in \mathbb{Z}$, mas o produto de 2 números inteiros é um número par se, e somente se, pelo menos um desses inteiros é par, logo $x \in 2\mathbb{Z}$ ou $y \in 2\mathbb{Z}$, portanto $2\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$.*

Definição 1.37. *Um ideal M de A é chamado de ideal maximal de A se $M \neq A$ e se não há nenhum outro ideal I de A tal que $M \subsetneq I \subsetneq A$.*

Exemplo 1.38. *O ideal $2\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, pois $2\mathbb{Z} \neq \mathbb{Z}$ e dado um ideal J de $\mathbb{Z}$ tal que $2\mathbb{Z} \subsetneq J$, então existe $x \in J$ tal que $x \notin 2\mathbb{Z}$, assim $x = 2n + 1$, para algum $n \in \mathbb{Z}$. Mas $x = 2n + 1$, logo $1 = x - 2n \in J$, e como $(1) = \mathbb{Z}$, temos que $J = \mathbb{Z}$.*

Proposição 1.39. *São válidas as seguintes afirmações:*

i) Um ideal P é um ideal primo de A se, e somente se, A/P é um domínio de integridade.

ii) Um ideal M é um ideal maximal de A se, e somente se, A/M é um corpo.

Demonstração. i) ($\Rightarrow$) Seja P um ideal primo de A e sejam $\overline{x}, \overline{y} \in A/P$, tais que $\overline{x \cdot y} = \overline{0}$, então $x \cdot y \in P$. Como P é um ideal primo de A, temos que $x \in P$ ou $y \in P$, logo $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Portanto, A/P é um domínio de integridade.

($\Leftarrow$) Seja A/P um domínio de integridade e sejam $x, y \in A$, tais que $x \cdot y \in P$. Como $x \cdot y \in P$, então $\overline{x \cdot y} = \overline{0}$ em A/P, e como A/P é um domínio de integridade, então $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Logo, $x \in P$ ou $y \in P$. Portanto, P é um ideal primo de A.

ii) ($\Rightarrow$) Seja M um ideal maximal de A. Como A é um anel com unidade, então A/M também é. Vamos mostrar que todo elemento não nulo de A/M é uma unidade. Seja $\overline{x} \in A/M$, com $\overline{x} \neq \overline{0}$, então $x \notin M$. Tomemos o ideal (x), temos que $M \subsetneq M + (x) \subseteq A$ (aqui estamos usando que a soma de ideais é um ideal, o que será provado na seção 1.6). Como M é um ideal maximal de A, então $M + (x) = A$, logo existem $y \in A$ e $z \in M$, tais que $1 = z + x \cdot y$, ou seja, $\overline{1} = \overline{z} + \overline{x \cdot y} = \overline{x} \cdot \overline{y}$. Assim, temos que $\overline{x}$ é uma unidade e portanto A/M é um corpo.

($\Leftarrow$) Seja A/M um corpo e seja I um ideal de A tal que $M \subsetneq I \subseteq A$. Então existe $x \in I$ tal que $x \notin M$, logo $\overline{x} \in A/M$ é tal que $\overline{x} \neq \overline{0}$. Como A/M é corpo, então existe $\overline{y} \in A/M$ tal que $\overline{1} = \overline{x} \cdot \overline{y}$, então $\overline{1} - \overline{x} \cdot \overline{y} = \overline{0}$, logo $1 - x \cdot y \in M$. Assim, existe $z \in M \subsetneq I$, tal que $1 - x \cdot y = z$, isto é $1 = z + x \cdot y$. Como $z \in I$ e $x \cdot y \in I$, temos que $1 \in I$, logo $I = A$. Portanto, M é um ideal maximal de A. □

Exemplo 1.40. *Todo ideal maximal é um ideal primo. De fato, se M é um ideal maximal de um anel A, então pelo item ii) da Proposição anterior, temos que A/M é um corpo. Pela Proposição 1.1, todo corpo é um domínio de integridade, logo A/M é um domínio de integridade. Pelo item i) da Proposição anterior, segue que M é um ideal primo de A.*

Exemplo 1.41. *Nem todo ideal primo é um ideal maximal. De fato, considere o ideal* $\{0\}$ *de* $\mathbb{Z}$. *Dados* $a, b \in \mathbb{Z}$ *tais que* $a \cdot b \in \{0\}$, *temos que* $a \cdot b = 0$ *e como* $\mathbb{Z}$ *é domínio de integridade, então* $a = 0$ *ou* $b = 0$, *ou seja,* $a \in \{0\}$ *ou* $b \in \{0\}$, *portanto* $\{0\}$ *é ideal primo de* $\mathbb{Z}$. *Mas* $\{0\}$ *não é ideal maximal de* $\mathbb{Z}$, *pois* $2\mathbb{Z}$ *é ideal de* $\mathbb{Z}$ *e* $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Proposição 1.42. *Seja* $f : A \to B$ *um homomorfismo de anéis e* P *um ideal primo de* B. *Então* $f^{-1}(P)$ *é um ideal primo de* A.

Demonstração. Sejam $x, y \in f^{-1}(P)$ e $z \in A$. Então $x, y \in A$ e $f(x), f(y) \in P$ e $f(z) \in B$. Como f é homomorfismo, temos que $0 \in f^{-1}(P)$ e como P é ideal de B, então $f(x) - f(y) \in P$, o que implica $f(x - y) \in P$, logo $x - y \in f^{-1}(P)$. Portanto $f^{-1}(P)$ é subgrupo aditivo de A. Além disso, $f(x) \cdot f(z) \in P$, o que implica $f(x \cdot z) \in P$, então $x \cdot z \in f^{-1}(P)$, logo $Af^{-1}(P) \subseteq f^{-1}(P)$. Portanto $f^{-1}(P)$ é ideal de A. Agora, sejam $k, l \in A$ tais que $k \cdot l \in f^{-1}(P)$. Então, $f(k \cdot l) = f(k) \cdot f(l) \in P$ e como P é ideal primo de B, então $f(k) \in P$ ou $f(l) \in P$, ou seja, $k \in f^{-1}(P)$ ou $l \in f^{-1}(P)$. Portanto, $f^{-1}(P)$ é ideal primo de A. □

Exemplo 1.43. *A Proposição anterior não é verdadeira se tomarmos um ideal maximal ao invés de um ideal primo. De fato, seja* $f : \mathbb{Z} \to \mathbb{Q}$ *o homomorfismo de inclusão. Como* $\mathbb{Q}$ *é um corpo, pelo item ii) da Proposição 1.3, temos que* $\{0\}$ *é ideal maximal de* $\mathbb{Q}$. *Como* f *é injetora, então* $f^{-1}\{0\} = \{0\}$, *que como vimos no Exemplo 1.41 não é um ideal maximal de* $\mathbb{Z}$.

Definição 1.44. *Seja* S *um conjunto não vazio parcialmente ordenado, isto é, existe uma relação* $x \leq y$ *em* S, *que é reflexiva e transitiva, e tal que se* $x \leq y$ *e* $y \leq x$, *temos* $x = y$. *Um subconjunto* T *de* S *é uma cadeia se* $x \leq y$ *ou* $y \leq x$ *para todos* $x, y \in T$.

Lema 1.45 (Lema de Zorn)**.** *Se toda cadeia* T *de* S *possui um limitante superior em* S, *então* S *possui ao menos um elemento maximal.*

Demonstração. A demonstração do Lema de Zorn é extensa e não será feita neste trabalho. Ela pode ser encontrada nas páginas 63, 64 e 65 da referência [4]. □

Teorema 1.46. *Todo anel* $A \neq 0$ *tem ao menos um ideal maximal.*

Demonstração. Seja S o conjunto de todos os ideais de A diferentes do próprio A. Em S considere a relação de ordem dada pela inclusão. S é não vazio, pois $0 \in S$. Vamos mostrar que toda cadeia em S tem um limitante superior em S. Seja (I_α) uma cadeia de ideais em S, então para cada par de indíces α, β nós temos que $I_\alpha \subseteq I_\beta$ ou que $I_\beta \subseteq I_\alpha$. Vamos supor, sem perda de generalidade, que $I_\beta \subseteq I_\alpha$. Seja $I = \bigcup_\alpha I_\alpha$. Vamos verificar que I é um ideal de A. Sejam $x, y \in I$, então existem índices α, β

tais que $x \in I_\alpha$ e $y \in I_\beta$. Como $0 \in I$ e por hipótese $I_\beta \subseteq I_\alpha$, então $x - y \in I_\alpha \subseteq I$. Portanto, I é subgrupo aditivo de A. Se $a \in A$, então $a \cdot x \in I_\alpha \subseteq I$, logo I é ideal de A. Além disso, $1 \notin I$ pois $1 \notin I_\alpha$, para todo α. Portanto, $I \in S$ e I é um limitante superior da cadeia (I_α). Assim, pelo Lema de Zorn, S tem um elemento maximal e, consequentemente, A possui ao menos um ideal maximal. □

Corolário 1.47. *Se $I \neq A$ é um ideal de A, então existe um ideal maximal de A contendo I.*

Demonstração. Pelo Teorema anterior, todo anel diferente de 0 tem pelo menos um ideal maximal, logo o anel A/I tem um ideal maximal. Pelo Teorema 1.18, há um correspondência biunívoca que preserva a ordem entre os ideais de A que contém I e os ideais de A/I. Portanto, existe um ideal maximal de A que contém I. □

Corolário 1.48. *Todo elemento não unidade de A está em um ideal maximal de A.*

Demonstração. Seja x um elemento não unidade de A, então o ideal $(x) \neq A$ e temos pelo Corolário anterior que (x) está contido em um ideal maximal M de A, logo $x \in M$. □

Definição 1.49. *Um anel A com um único ideal maximal M é chamado de anel local e o corpo $K = A/M$ é chamado corpo residual. Um anel com um número finito de ideais maximais é chamado de anel semi-local.*

Exemplo 1.50. *Todo corpo é um anel local. De fato, pela Proposição 1.2 sabemos que os únicos ideais de um corpo K são 0 e K. Portanto, 0 é o único ideal maximal de K.*

Proposição 1.51. *São válidas as seguintes afirmações:*

i) Seja A um anel e $M \neq A$ um ideal de A tal que todo $x \in A - M$ é uma unidade em A. Então A é um anel local e M é seu ideal maximal.

ii) Seja A uma anel e M um ideal maximal de A tal que todo elemento de $1 + M = \{1 + t : t \in M\}$ é uma unidade em A. Então A é um anel local.

Demonstração. *i*) Todo ideal $I \neq A$ consiste de não unidades e então estão contidos em M. Assim, M é o único ideal maximal de A, portanto A é um anel local.

ii) Seja $x \in A - M$. Como M é maximal e $M \subsetneq (x) + M \subseteq A$, então $(x) + M = A$, onde $(x) + M$ é o ideal gerado por x e M. Daí existem $y \in A$ e $t \in M$ tais que $x \cdot y + t = 1$, então $x \cdot y = 1 - t \in 1 + M$ e assim, por hipótese, $x \cdot y$ é uma unidade em A. Portanto, x é uma unidade em A e então, pelo item (i), A é anel local. □

1.5 Nilradical e radical de Jacobson

Definição 1.52. *O conjunto de todos os elementos nilpotentes em um anel A é chamado de nilradical de A e é denotado por $\mathcal{N}(A)$.*

Proposição 1.53. *O nilradical de um anel A é um ideal de A e $A/\mathcal{N}(A)$ não possui nenhum elemento nilpotente não nulo.*

Demonstração. Vamos verificar que $\mathcal{N}(A)$ é um ideal de A:

- $\mathcal{N}(A) \neq \emptyset$, pois $0^n = 0$, para todo $n \in \mathbb{Z}$, com $n > 0$, logo $0 \in \mathcal{N}(A)$.
- Sejam $x, y \in \mathcal{N}(A)$, então existem inteiros positivos n e m, tais que $x^m = 0$ e $y^n = 0$. Assim $(x+y)^{n+m-1}$ é a soma dos inteiros múltiplos de produtos $x^r y^s$, onde $r + s = m + n - 1$, isto é

  $$(x+y)^{m+n-1} = x^{m+n-1} + \binom{m+n-1}{1} \cdot x^{m+n-2} + \ldots + \binom{m+n-1}{m+n-2} \cdot x \cdot y^{m+n-2} + y^{m+n-1}.$$

  Como não podemos ter $r < m$ e $s < n$, cada uma destas parcelas se anula, e assim temos que $(x+y)^{m+n-1} = 0$. Portanto $x + y \in \mathcal{N}(A)$.
- Se $x \in \mathcal{N}(A)$, então existe um inteiro positivo n, tal que $x^n = 0$. Se n for par, então $(-x)^n = x^n = 0$, e se n for ímpar, então $(-x^n) = -(x^n) = 0$. Portanto $-x \in \mathcal{N}(A)$.
- Se $x \in \mathcal{N}(A)$ e $y \in A$, então existe um inteiro positivo n, tal que $(y \cdot x)^n = y^n \cdot x^n = y^n \cdot 0 = 0$. Logo, $x \cdot y \in \mathcal{N}(A)$.

Portanto, $\mathcal{N}(A)$ é ideal de A.
Agora, vamos mostras que $A/\mathcal{N}(A)$ não possui nenhum elemento nilpotente não nulo. Seja $\overline{x} \in A/\mathcal{N}(A)$ representado por $x \in A$ e $\overline{x}^i$ representado por x^i, então existe um inteiro positivo n, tal que $\overline{x}^n = \overline{0}$, o que implica $x^n \in \mathcal{N}(A)$, logo $(x^n)^k = 0$, para algum $k > 0$. Mas $(x^n)^k = 0$, o que implica $x^{nk} = 0$, logo $x \in \mathcal{N}(A)$, e então $\overline{x} = \overline{0}$. Portanto, se $\overline{x}$ é um elemento nilpotente de $A/\mathcal{N}(A)$, então $\overline{x}$ é nulo. □

Proposição 1.54. *O nilradical de um anel A é a interseção de todos os ideais primos de A.*

Demonstração. Seja $\bigcap_i P_i$ a interseção de todos os ideais primos de A. Se $f \in \mathcal{N}(A)$ e se P é um ideal primo de A, então $f^n = 0 \in P$, para algum inteiro $n > 0$. Logo, $f \in P$, pois P é primo. Assim, $f \in \bigcap_i P_i$. Portanto, $\mathcal{N}(A) \subseteq \bigcap_i P_i$.

Provaremos a inclusão contrária pela contra-positiva. Suponha que $f \notin \mathcal{N}(A)$, ou seja, que f não é nilpotente. Seja S o conjunto dos ideais I com a propriedade de que $n > 0$ implica $f^n \notin I$. Então

S é não vazio, pois $0 \in S$. O Lema de Zorn aplicado ao conjunto S, ordenado pela inclusão, garante que S tem um elemento maximal. Seja P esse elemento maximal de S. Vamos mostrar que P é um ideal primo. Sejam $x, y \notin P$. Então os ideais $P + (x), P + (y)$ contêm P estritamente e assim não pertencem a S. Logo $f^m \in P + (x)$ e $f^n \in P + (y)$, para certos inteiros positivos m e n. Segue que $f^{m+n} \in P + (x \cdot y)$, e então o ideal $P + (x \cdot y)$ não pertence a S e daí $x \cdot y \notin P$. Assim temos um ideal primo P tal que $f \notin P$, e portanto $f \notin \bigcap_i P_i$. Logo, se $f \in \bigcap_i P_i$, então $f \in \mathcal{N}(A)$, ou seja, $\bigcap_i P_i \subseteq \mathcal{N}(A)$. Portanto $\mathcal{N}(A) = \bigcap_i P_i$. □

Definição 1.55. *A interseção de todos os ideais maximais de um anel A é chamada de radical de Jacobson e denotada por $\mathcal{J}$.*

Proposição 1.56. *O Radical de Jacobson de um anel A pode ser caracterizado da seguinte forma: $x \in \mathcal{J} \Leftrightarrow 1 - x \cdot y$ é uma unidade em A, para todo $y \in A$.*

Demonstração. ($\Rightarrow$) Suponha que $x \in \mathcal{J}$ e que $1 - x \cdot y$ não seja um elemento unidade em A. Pelo Corolário 1.2, toda não unidade está em um ideal maximal, logo $1 - x \cdot y$ pertence a um ideal maximal M de A. Mas $x \in \mathcal{J} \subseteq M$, logo $x \in M$ e portanto $x \cdot y \in M$. Mas se $1 - x \cdot y \in M$ e $x \cdot y \in M$, então $1 \in M$ e então $M = A$, o que é um absurdo. Portanto, $1 - x \cdot y$ é uma unidade em A.

($\Leftarrow$) Vamos provar pela contra-positiva. Suponha $x \notin M$ para algum ideal maximal M, então $x \notin \mathcal{J}$. Como M é ideal maximal de A, temos que M e x geram o ideal $(1) = A$, e temos $u + xy = 1$ para algum $u \in M$ e algum $y \in A$. Como $u \in M$ e $u = 1 - x \cdot y$, então $1 - x \cdot y \in M$ e portanto não é uma unidade de A. □

1.6 Operações com ideais

Definição 1.57. *Sejam I e J ideais de um anel A, definimos a soma $I + J = \{x + y : x \in I \text{ e } y \in J\}$. De forma geral, definimos a soma $\sum_{j \in I} I_j$ para qualquer família de ideais I_j de A. Seus elementos são todas as somas finitas $\sum x_j$, onde $x_j \in I_j$, para todo $j \in I$.*

Proposição 1.58. *A soma $\sum_{j \in I} I_j$ é o menor ideal de A contendo todos os I_j.*

Demonstração. Sejam $x, y \in \sum_{j \in I} I_j$. Então $x = \sum_{j \in I} x_j$ e $y = \sum_{j \in I} y_j$, com $x_j, y_j \in I_j$, para todo $j \in I$. Logo, $x - y = \sum_{j \in I} x_j - \sum_{j \in I} y_j = \sum_{j \in I} x_j - y_j$. Como I_j é ideal, temos que $x_j - y_j \in I_j$, para todo $j \in I$, portanto $x - y \in \sum_{j \in I} I_j$. Seja $z \in \sum_{j \in I} I_j$, então $z = \sum_{j \in I} z_j$, com $z_j \in I_j$ e, para todo $a \in A$, temos que $az = a \sum_{j \in I} z_j = \sum_{j \in I} az_j$. Como I_j é ideal, então $az_j \in I_j$, para todo $j \in I$, portanto $az \in \sum_{j \in I} I_j$. Logo, $A \sum_{j \in I} \subseteq \sum_{j \in I}$. Concluímos assim que $\sum_{j \in I}$ é um ideal. Agora, seja J um ideal contendo todos os I_j. Como ideais são fechados pela adição, então $\sum_{j \in I} I_j \subseteq J$. Portanto, $\sum_{j \in I} I_j$ é o menor ideal de A contendo todos os I_j. □

Definição 1.59. *Sejam I e J ideais de um anel A, definimos a interseção $I \cap J = \{x \in A : x \in I \text{ e } x \in J\}$. Da mesma forma, definimos a interseção de qualquer família de ideais.*

Proposição 1.60. *A interseção de qualquer família $(I_j)_{j\in I}$ de ideais é um ideal.*

Demonstração. Sejam $x, y \in \bigcap_{j\in I} I_j$. Então $x, y \in I_j$ para todo j, portanto $x - y \in I_j$, para todo j, ou seja, $x - y \in \bigcap_{j\in I} I_j$. Seja $z \in \bigcap_{j\in I} I_j$, então $z \in I_j$, para todo j. Como I_j é ideal, então para todo $a \in A$, temos que $az \in I_j$, para todo j, ou seja $az \in \bigcap_{j\in I} I_j$. Logo, $A\bigcap_{j\in I} I_j \subseteq \bigcap_{j\in I} I_j$. Concluímos assim que $\bigcap_{j\in I} I_j$ é um ideal. □

Definição 1.61. *Sejam I e J ideais de um anel A, definimos o produto IJ como o conjunto formado por todas as somas finitas $\sum x_i y_i$, onde cada $x_i \in I$ e cada $y_i \in J$. Da mesma forma, definimos o produto de qualquer família finita de ideais. Em particular, as potências $I^n, n > 0$, de um ideal I estão definidas. Convenientemente, $I^0 = (1) = A$, e então $I^n, n > 0$, é o ideal gerado por todos os produtos $x_1x_2...x_n$, no qual cada fator x_i pertence a I.*

Proposição 1.62. *O produto de qualquer família finita $(I_j)_{j=1,\cdots,n}$, de ideais também é um ideal.*

Demonstração. A demonstração deste resultado não será feita neste trabalho e pode ser encontrada na referência [1]. □

Observação 1.63. *As operações soma, interseção e produto com ideais, são associativas e comutativas.*

Exemplo 1.64. *Se $A = \mathbb{Z}$, $I = (m)$ e $J = (n)$, então $I + J$ é o ideal gerado pelo máximo divisor comum de m e n. A interseção $I \cap J$ é o ideal gerado pelo mínimo múltiplo comum de m e n. O produto $IJ = (mn)$. Neste caso, temos que $IJ = I \cap J$ se, e somente se, m e n são primos entre si, pois neste caso o mínimo múltiplo comum de a e b é ab.*

Exemplo 1.65. *Sejam I, J, K ideais de um anel A, então vale a lei distributiva $I(J+K) = IJ+IK$. De fato, como $J \subseteq J + K$, então $IJ \subseteq I(J + K)$, e como $K \subseteq J + K$, então $IK \subseteq I(J + K)$. Logo, $IJ + IK \subseteq I(J + K)$. Por outro lado, se $x \in I(J + K)$, então $x = \sum_i x_i(y_i + z_i)$, com $x_i \in I$, $y_i \in J$ e $z_i \in K$. Logo, $x = \sum_i x_i y_i + \sum_i x_i z_i$, e então $x \in IJ + IK$ e então $I(J + K) \subseteq IJ + IK$. Portanto, $I(J + K) = IJ + IK$.*

Exemplo 1.66. *Sejam I, J, K ideais de um anel A, então $(I \cap J) + (I \cap K) \subseteq I \cap (J + K)$. De fato, como $(I \cap J) \subseteq I$ e $(I \cap K) \subseteq I$, temos que $(I \cap J) + (I \cap K) \subseteq I$. Da mesma forma, como $(I \cap J) \subseteq J$ e $(I \cap K) \subseteq K$, temos que $(I \cap J) + (I \cap K) \subseteq (J + K)$. Portanto, $(I \cap J) + (I \cap K) \subseteq I \cap (J + K)$.*

Exemplo 1.67. *Sejam I, J, K ideais de um anel A tais que $J \subseteq I$ ou $K \subseteq I$, então $I \cap (J + K) = (I \cap J) + (I \cap K)$. De fato, seja $x \in I \cap (J + K)$, então $x \in I$ e $x \in J + K$, logo existem $j \in J$ e $k \in K$, tais que $x = j + k$. Queremos mostrar que $x \in (I \cap J) + (I \cap K)$. Se $J \subseteq I$, então $(I \cap J) + (I \cap K) = J + (I \cap K)$. Sabemos que $j \in J$, resta mostrar que $k \in I \cap K$. De fato, $k \in K$ e também $k \in I$, pois $x = j + k$, o que implica $x - j = k$, logo $k \in I$ pois $x \in I$ e $j \in I$. Portanto, $I \cap (J + K) \subseteq (I \cap J) + (I \cap K)$, e como a inclusão contrária é sempre verdade pelo Exemplo anterior, então vale a igualdade. Se assumirmos que $K \subseteq I$ o resultado é análogo.*

Definição 1.68. *Sejam I e J ideais de um anel A. Dizemos que I e J são ideais coprimos se $I + J = (1) = A$. Dessa forma, dois ideais I, J são coprimos se, e somente se, existem $i \in I$ e $j \in J$ tais que $i + j = 1$.*

Proposição 1.69. *Se I e J são ideais coprimos de um anel A, então $I \cap J = IJ$.*

Demonstração. Sejam I e J ideais coprimos de A. Então, existem $i \in I$ e $j \in J$ tais que $i + j = 1$. Seja $x \in I \cap J$, então $x = x \cdot 1 = x \cdot (i + j) = xi + xj \in IJ$, pois $xi \in IJ$, $xj \in IJ$ e IJ é ideal pela Proposição 1.62. Logo, $I \cap J \subseteq IJ$. Seja $y \in IJ$, então $y = ab$, onde $a \in I$ e $b \in J$. Como I e J são ideais, então $ab \in I$ e $ab \in J$, logo $x = ab \in I \cap J$, Logo, $IJ \subseteq I \cap J$. Portanto, $I \cap J = IJ$, como queríamos provar. □

Definição 1.70. *Sejam $A_1, A_2, ..., A_n$ anéis. O produto direto $A = \prod_{i=1}^{n} A_i$ é o conjunto de todas as sequências $x = (x_1, x_2, ..., x_n)$, com $x_i \in A_i$, com adição e multiplicação definidas componente a componente. A é um anel comutativo com elemento identidade $(1, ..., 1)$. Temos as projeções $p_i : A \to A_i$, definidas por $p_i(x) = x_i$, que são homomorfismos de anéis.*

Proposição 1.71. *Sejam A um anel e $I_1, ..., I_n$ ideais de A. Definimos o homomorfismo $\phi : A \to \prod_{i=1}^{n}(A/I_i)$ pela regra $\phi(x) = (x + I_1, ..., x + I_n)$. Para este homomorfismo, temos que:*

i) Se I_i e I_j são coprimos sempre que $i \neq j$, então $\prod I_i = \bigcap I_i$.

ii) ϕ é sobrejetor se, e somente se, I_i e I_j são coprimos sempre que $i \neq j$.

iii) ϕ é injetor se, e somente se, $\bigcap I_i = 0$.

Demonstração. *i)* Provaremos por indução sobre n. Já vimos que o reultado vale para $n = 2$. Suponha $n > 2$ e que o resultado seja válido para $I_1, ..., I_{n-1}$ e seja $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Como os ideias são coprimos, por hipótese, temos que $I_i + I_n = (1)$ para $1 \leq i \leq n - 1$. Então existem equações do tipo $x_i + y_i = 1$, onde $x_i \in I_i$ e $y_i \in I_n$. Portanto

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1 - y_i) = 1 - \alpha \equiv 1 \ (mod\ I_n),$$

para algum $\alpha \in I_n$. Como $\prod_{i=1}^{n-1} x_i = x \in J$ e $x = 1 - \alpha$, então $x + \alpha = 1$, logo I_n e J são coprimos. Portanto, $\prod_{i=1}^{n} I_i = J \cdot I_n = J \cap I_n = \bigcap_{i=1}^{n} I_i$.

ii) ($\Rightarrow$) Sem perda de generalidade, vamos provar que I_1 e I_2 são coprimos. Suponha que o homomorfimo $\phi : A \to \prod_{i=1}^{n}(A/A_i)$ tal que $\phi(x) = (x + I_1, ..., x + I_n)$ seja sobrejetor. Então existe $x \in A$ tal que $\phi(x) = (\overline{1}, \overline{0}, ..., \overline{0})$. Portanto $x \equiv 1 \ (mod\ I_1)$ e $x \equiv 0 \ (mod\ I_2)$, então $1 = (1 - x) + x \in (I_1 + I_2)$.

($\Leftarrow$) É suficiente mostrar, por exemplo, que existe um elemento $x \in A$ tal que $\phi(x) = (\overline{1}, \overline{0}, ..., \overline{0})$. Como, por hipótese, $I_1 + I_i = (1)$, com $i > 1$, temos equações $u_i + v_i = 1$, com $u_i \in I_1$ e $v_i \in I_i$. Tomemos $x = \prod_{i=2}^{n} v_i$, então $x = \prod(1 - u_i) \equiv 1 \ (mod\ I_1)$ e $x \equiv 0 \ (mod\ I_i)$, com $i > 1$. Portanto $\phi(x) = (\overline{1}, \overline{0}, ..., \overline{0})$ como queríamos mostrar.

iii) Temos que $x \in ker(\phi)$ se, e somente se, $x \equiv 0 \ (mod\ I_i)$, com $i = 1, ..., n$ se, e somente se, $x \in \bigcap I_i$. Logo, $ker(\phi) = \bigcap I_i$. Portanto, ϕ é injetora se, e somente se, $\bigcap I_i = 0$.

□

Observação 1.72. *A união $I \cup J$ de dois ideais de um anel A, em geral, não é um ideal de A. Por exemplo, no anel $\mathbb{Z}$, temos os ideais (2) e (7), mas o conjunto $(2) \cup (7)$ não é um subgrupo aditivo de $\mathbb{Z}$, pois $7, 2 \in (2) \cup (7)$ mas $5 = 7 - 2 \notin (2) \cup (7)$. Portanto, não é um ideal de $\mathbb{Z}$. Porém, quando os ideais I e J são primos, podemos provar alguns resultados conforme a Proposição a seguir.*

Proposição 1.73. *São válidas as seguintes afirmações:*

i) Sejam $P_1, ..., P_n$ ideais primos e I um ideal contido em $\bigcup_{i=1}^{n} P_i$. Então $I \subseteq P_i$, para algum i.

ii) Sejam $I_1, ..., I_n$ ideais e seja P um ideal primo contendo $\bigcap_{i=1}^{n} I_i$. Então $I_i \subseteq P$ para algum i. Se $P = \bigcap I_i$, então $P = I_i$ para algum i.

Demonstração. *i)* Provaremos por indução sobre n a contra-recíproca do resultado, ou seja, que se $I \not\subseteq P_i$, para todo $1 \leq i \leq n$, então $I \not\subseteq \bigcup_{i=1}^{n} P_i$. Claramente, o resultado é válido para $n = 1$. Suponhamos $n > 1$ e que o resultado seja verdadeiro para $n - 1$. Então, pela hipótese de indução, para cada i existe $x_i \in I$ tal que $x_i \notin P_j$, sempre que $i \neq j$. Se para algum i tivermos $x_i \notin P_i$, o resultado está provado. Se $x_i \in P_i$ para todo i, consideremos o elemento $y = \sum_{i=1}^{n} x_1 x_2 ... x_{i-1} x_{i+1} x_{i+2} ... x_n$. Pela escolha dos x_i, temos que $y \in I$ e $y \notin P_i$, com $1 \leq i \leq n$. Portanto, $I \not\subseteq \bigcup_{i=1}^{n} P_i$.

ii) Provaremos a contra-recíproca do resultado, ou seja, que se $I_i \not\subseteq P$, para todo i, então $\bigcap_{i=1}^{n} I_i \not\subseteq P$. Suponha que $I_i \not\subseteq P$, então existe $x_i \in I_i$, tal que $x_i \notin P$, com $1 \leq i \leq n$, e assim

$\prod x_i \in \prod I_i \subseteq \bigcap I_i$. Mas $\prod x_i \notin P$, pois P é primo. Portanto $\bigcap_{i=1}^{n} I_i \not\subseteq P$. Além disso, se $P = \bigcap I_i$, então $P \subseteq I_i$, e portanto $P = I_i$ para algum i.

□

Definição 1.74. *Se I e J são ideais em um anel A, o ideal quociente é definido como $(I : J) = \{x \in A : x \cdot y \in I, \forall y \in J\}$. Em particular, $(0 : J) = \{x \in A : x \cdot y = 0, \forall y \in J\}$ é chamado de anulador de J e também denotado por $Ann(J)$. Nesta notação, o conjunto de todos os divisores de zero em A é $D = \bigcup_{x \neq 0} Ann(x)$. Se J é um ideal principal (x), escrevemos $(I : x)$ ao invés de $(I : (x))$.*

Exemplo 1.75. *Se $A = \mathbb{Z}$, $I = (3)$ e $J = (2)$, então o ideal quociente $(3 : 2) = \{x \in \mathbb{Z} : x \cdot 2m = 3n$; para todo m e algum $n \in \mathbb{Z}\} = (3)$, enquanto o anulador $Ann(2) = \{x \in \mathbb{Z} : x \cdot 2m = 0$; para todo $m \in \mathbb{Z}\} = \{0\}$.*

Proposição 1.76. *Sejam I e J ideais de um anel A. Então o ideal quociente $(I : J)$ é um ideal de A.*

Demonstração. Sejam $x, y \in (I : J)$. Então $xJ \subseteq I$ e $yJ \subseteq I$. Seja $j \in J$. Temos que $(x + y)j = xj + yj \in I$, pois I é ideal. Como j é arbitrário, temos que $(x + y)J \subseteq I$. Portanto, $x + y \in (I : J)$. Agora, sejam $x \in (I : J), y \in A$ e $j \in J$. Temos que $xyj = (xj)y \in I$, pois I é ideal. Como j é arbitrário, temos que $xyJ \subseteq I$, logo $xy \in (I : J)$. assim, para todo $y \in A$ e para todo $x \in (I : J)$, temos que $xy \in (I : J)$, logo $A(I : J) \subseteq (I : J)$. Portanto, $(I : J)$ é ideal de A. □

Proposição 1.77. *Sejam I, J e K ideais de um anel A. São válidas as seguintes propriedades:*

i) $I \subseteq (I : J)$;

ii) $(I : J)J \subseteq I$;

iii) $((I : J) : K) = (I : JK) = ((I : K) : J)$;

iv) $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$;

v) $(I : \sum_i J_i) = \bigcap_i (I : J_i)$.

Demonstração. *i)* Seja $i \in I$. Como I é ideal, temos que $ix \in I$, para todo $x \in A$, em particular, $ij \in I$, para todo $j \in J$, logo $iJ \subseteq I$ e então $i \in (I : J)$. Portanto, $I \subseteq (I : J)$.

ii) Seja $x \in (I : J)J$. Então $x = yj$, onde $y \in (I : J)$ e $j \in J$. Como $y \in (I : J)$, então $yz \in I$, para todo $z \in J$. Como $j \in J$, então $x = yj \in I$. Portanto, $(I : J)J \subseteq I$.

iii) Vamos provar a primeira igualdade, a segunda igualdade segue diretamente da primeira. Temos que

$$x \in ((I:J):K) \Leftrightarrow xk \in (I:J), \forall k \in K \Leftrightarrow xkj \in I, \forall k \in K, \forall j \in J \Leftrightarrow x \in (I:JK).$$

Logo $((I:J):K) = (I:JK)$.

iv) Temos que

$$x \in (\bigcap_i I_i : J) \Leftrightarrow xj \in \bigcap_i I_i, \forall j \in J \Leftrightarrow xj \in I_i, \forall i, \forall j \in J \Leftrightarrow x \in (I_i:J), \forall i \Leftrightarrow x \in \bigcap_i (I_i:J).$$

Logo $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$.

v) Temos que

$$x \in (I : \sum_i J_i) \Leftrightarrow xy \in I, \forall y \in \sum_i J_i \Leftrightarrow xz \in I, \forall z \in J_i, \forall i \Leftrightarrow x \in (I:J_i), \forall i \Leftrightarrow x \in \bigcap_i (I:J_i).$$

Logo $(I : \sum_i J_i) = \bigcap_i (I : J_i)$.

□

Definição 1.78. *Se I é ideal de um anel A, definimos o radical de I como o conjunto $Rad(I) = \{x \in A : x^n \in I$ para algum $n > 0\}$.*

Proposição 1.79. *Se $\phi : A \to A/I$ é a projeção canônica de A em A/I, então $Rad(I) = \phi^{-1}(\mathcal{N}(A/I))$.*

Demonstração. De fato, temos que $\mathcal{N}(A/I) = \{\overline{x} \in A/I : \overline{x}^n = \overline{x^n} = \overline{0}$, para algum $n > 0\}$. Assim, $\phi^{-1}(\mathcal{N}(A/I)) = \{x \in A : x^n \in I$, para algum $n > 0\} = Rad(I)$. □

Proposição 1.80. *Sejam I e J ideais de um anel A. São válidas as seguintes propriedades:*

i) $I \subseteq Rad(I)$;

ii) $Rad(Rad(I)) = Rad(I)$;

iii) $Rad(IJ) = Rad(I \cap J) = Rad(I) \cap Rad(J)$;

iv) $Rad(I) = (1) \Leftrightarrow I = (1)$;

v) $Rad(I) + Rad(J) \subseteq Rad(I + J)$;

vi) $Rad(I + J) = Rad(Rad(I) + Rad(J))$;

vii) *Se P é um ideal primo, então $Rad(P^n) = P$, para todo $n > 0$.*

Demonstração. *i)* Seja $x \in I$, então $x^1 \in I$, logo $x \in Rad(I)$. Portanto, $I \subseteq Rad(I)$.

ii) Pelo item *i)*, temos que $Rad(I) \subseteq Rad(Rad(I))$. Vamos mostrar que $Rad(Rad(I)) \subseteq Rad(I)$. De fato, seja $x \in Rad(Rad(I))$, então $x^n \in Rad(I)$, o que implica $(x^n)^m \in I$, logo $x^{nm} \in I$, e portanto $x \in Rad(I)$.

iii) Provemos a primeira igualdade. Como $IJ \subseteq I \cap J$, então $Rad(IJ) \subseteq Rad(I \cap J)$. Vamos mostrar a inclusão contrária. Seja $x \in Rad(I \cap J)$, então $x^n \in I \cap J$, logo $x^n \in I$ e $x^n \in J$, para algum inteiro positivo n. Daí, $x^n \cdot x^n = x^{2n} \in IJ$, e então $x \in Rad(IJ)$. Logo, $Rad(I \cap J) \subseteq Rad(IJ)$, portanto $Rad(IJ) = Rad(I \cap J)$.

Agora, vamos provar a segunda igualdade. Temos que $Rad(I \cap J) = \{x \in A : x^n \in I \cap J\} = \{x \in A : x^n \in I \; e \; x^n \in J\} = \{x \in A : x^n \in I\} \cap \{x \in A : x^n \in J\} = Rad(I) \cap Rad(J)$.

iv) Suponha que $Rad(I) = (1)$, então $1 \in Rad(I)$. Logo, existe um inteiro positivo n tal que $1^n \in I$. Mas $1^n = 1$, para todo n. Assim, $1 \in I$ e portanto $I = (1)$. Por outro lado, pelo item $i)$ temos que $I \subseteq Rad(I)$, se $I = (1)$ então $Rad(I) = 1$.

v) Seja $x \in Rad(I)$ e $y \in Rad(J)$, então $x + y \in Rad(I) + Rad(J)$. Como $x \in Rad(I)$, então $x \in Rad(I + J)$ e como $y \in Rad(J)$, então $y \in Rad(I + J)$. Como $Rad(I + J)$ é ideal, então $x + y \in Rad(I + J)$. Logo, $Rad(I) + Rad(J) \subseteq Rad(I + J)$.

vi) Como $I \subseteq Rad(I)$ e $J \subseteq Rad(J)$, então $I + J \subseteq Rad(I) + Rad(J)$, logo $Rad(I + J) \subseteq Rad(Rad(I)+Rad(J))$. Pelo item $v)$, temos que $Rad(I)+Rad(J) \subseteq Rad(I+J)$, logo $Rad(Rad(I)+Rad(J)) \subseteq Rad(Rad(I + J)) = Rad(I + J)$. Portanto, $Rad(I + J) = Rad(Rad(I) + Rad(J))$.

vii) Seja $x \in P$, então $x^n \in P^n \subseteq Rad(P^n)$. Logo $P \subseteq Rad(P^n)$. Por outro lado, se $x \in Rad(P^n)$, então $x^m \in P^n$, para algum $m > 0$. Como $P^n \subseteq P$, então $x^m \in P$ e já que P é ideal primo, vem que $x \in P$. Logo $Rad(P^n) \subseteq P$. Portanto, $P = Rad(P^n)$.

□

Proposição 1.81. *O radical de um ideal I de um anel A é a interseção dos ideias primos de A que contêm I.*

Demonstração. Pela Proposição 1.53, o nilradical de A/I é a interseção de todos os ideais primos de A/I. Se $\overline{P}$ é um ideal primo de A/I, então $P = \phi^{-1}(\overline{P})$ é um ideal primo de A que contém I, pois pelo Teorema da Correspondência entre Ideais existe uma correspondência biunívoca que preserva a ordem entre os ideais J de A que contém I e os ideais $\overline{J}$ de A/I. Então, $Rad(I) = \phi^{-1}(\mathcal{N}_{\mathcal{A}/\mathcal{I}}) = \bigcap \phi^{-1}(\overline{P}) = \bigcap P$, onde $\mathcal{N}_{\mathcal{A}/\mathcal{I}}$ é o nilradical de A/I. □

Definição 1.82. *Defnimos o radical $Rad(E)$ de qualquer subconjunto E de um anel A que, em geral, não é um ideal. Temos $Rad(\bigcup_\alpha E_\alpha) = \bigcup Rad(E_\alpha)$ para qualquer família de subconjuntos E_α de A.*

Proposição 1.83. *Seja D o conjunto dos divisores de zero do anel A. Então $D = \bigcup_{x\neq 0} Rad(Ann(x))$.*

Demonstração. Sabemos pelo item i) da Proposição 1.69 que $D \subseteq Rad(D)$. Vamos mostrar que $Rad(D) \subseteq D$ e portanto vale a igualdade. Seja $x \in Rad(D)$, então $x^n \in D$, para algum $n > 0$. Suponha que n seja o menor inteiro com esta propriedade, ou seja, $x^{n-1} \notin D$. Temos que $x^n y = x \cdot x^{n-1} \cdot y = x(x^{n-1}y) = 0$, para algum $y \in A$, com $y \neq 0$. Logo $x \in D$. Então $Rad(D) \subseteq D$, logo $D = Rad(D)$. Portanto, temos que $D = Rad(D) = Rad(\bigcup_{x\neq 0} Ann(x)) = \bigcup_{x\neq 0} Rad(Ann(x))$. □

Proposição 1.84. *Sejam I e J ideais de um anel A tais que $Rad(I)$ e $Rad(J)$ são coprimos. Então I e J são coprimos.*

Demonstração. Como $Rad(I)$ e $Rad(J)$ são coprimos, então $Rad(I)+Rad(J) = (1)$. Logo, $Rad(Rad(I)+Rad(J)) = Rad(1) = (1)$. Pelo item v) da Proposição 1.69, temos que $Rad(Rad(I) + Rad(J)) = Rad(I + J)$, logo $Rad(I + J) = (1)$. Pelo item iv) da Proposição 1.69, temos que $I + J = (1)$. Portanto, I e J são coprimos. □

1.7 Extensão e contração de ideais

Definição 1.85. *Seja $f : A \to B$ um homomorfismo de anéis e I um ideal de A. Definimos a extensão I^e de I como sendo o ideal $Bf(I)$ gerado por $f(I)$ em B. Explicitamente:*

$$I^e := \left\{ \sum y_i f(x_i) : x_i \in I \text{ e } y_i \in B \right\}.$$

Definição 1.86. *Seja $f : A \to B$ um homomorfismo de anéis e J um ideal de B. Definimos a contração J^c de J como sendo o ideal $f^{-1}(J)$.*

Proposição 1.87. *Sejam $f : A \to B$ um homomorfismo de anéis e J_1, J_2 ideais de B. Vale que $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.*

Demonstração. Como $J_1 \cap J_2 \subseteq J_1$, então $(J_1 \cap J_2)^c \subseteq J_1^c$ e como $J_1 \cap J_2 \subseteq J_2$, então $(J_1 \cap J_2)^c \subseteq J_2^c$. Logo, $(J_1 \cap J_2)^c \subseteq J_1^c \cap J_2^c$. Por outro lado, seja $x \in J_1^c \cap J_2^c$, então $x \in J_1^c$ e $x \in J_2^c$, isto é, $x \in f^{-1}(J_1)$ e $x \in f^{-1}(J_2)$. Logo, $f(x) \in J_1$ e $f(x) \in J_2$, então $f(x) \in J_1 \cap J_2$, e portanto $x \in f^{-1}(J_1 \cap J_2)$. Logo $J_1^c \cap J_2^c \subseteq (J_1 \cap J_2)^c$. Portanto, vale a igualdade. □

Capítulo 2

Módulos

Neste capítulo, iremos ampliar nossos estudos para os módulos, generalizando o que vimos até aqui para ideais. Desta forma, iremos apresentar os conceitos, propriedades e resultados básicos sobre homomorfismos de módulos, submódulos, módulos quocientes e uma aplicação no estudo de sequências exatas.

2.1 Módulos e homomorfismos de módulos

Definição 2.1. *Dado um anel A, um A-módulo é um grupo abeliano $(M, +)$ em que A age linearmente, isto é, um par (M, μ), onde μ é uma função de $A \times M$ em M tal que, para cada par $(a, m) \in A \times M$, associa um elemento $a \cdot m \in M$ de forma que para quaisquer $a, b \in A$ e $x, y \in M$, é verdade que:*

$$a \cdot (x + y) = ax + ay,$$

$$(a + b) \cdot x = a \cdot x + b \cdot x,$$

$$(ab) \cdot x = a \cdot (bx),$$

$$1 \cdot x = x.$$

Definição 2.2. *Dados dois A-módulos M e N, uma função $f : M \to N$ é chamada de A-homomorfismo ou homomorfismo de A-módulos se, para quaisquer $x, y \in M$ e $a \in A$, for verdade que:*

$$f(x + y) = f(x) + f(y),$$

$$f(a \cdot x) = a \cdot f(x).$$

Proposição 2.3. *A composição de homomorfismos de A-módulos é ainda um homomorfismo de A-módulos.*

Demonstração. Sejam M, N e Q A-módulos, $f : M \to N$ e $g : N \to Q$ homomorfismos de A-módulos, $x, y \in M$ e $a \in A$, então

$$(g \circ f)(x + y) = g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) = (g \circ f)(x) + (g \circ f)(y) \quad e$$
$$(g \circ f)(a \cdot x) = g(f(a \cdot x)) = g(a \cdot f(x)) = a \cdot g(f(x)) = a \cdot (g \circ f)(x).$$

Portanto $g \circ f$ é um homomorfismo de A-módulos. □

Observação 2.4. *Pode-se verificar também que a soma $f + g$ de homomorfismos de A-módulos e que o produto af de um elemento do anel por um A-módulo também é ainda um homomorfismo de A-módulos.*

Considere o conjunto de todos os homomorfismos de A-módulos de M em N, que denotamos por $Hom(M, N)$. Para todo $a \in A$ e $x \in M$ definimos $f + g$ e $a \cdot f$ pelas regras:

$$(f + g)(x) = f(x) + g(x),$$
$$(a \cdot f)(x) = a \cdot f(x).$$

Proposição 2.5. *O conjunto $Hom(M, N)$ é um A-módulo.*

Demonstração. Vamos mostrar que $Hom(M, N)$ é um grupo abeliano. De fato, dado $x \in M$, temos que:

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x),$$
$$(f + (g + h))(x) = f(x) + (g + h)(x) = f(x) + g(x) + h(x) = (f + g)(x) + h(x) = ((f + g) + h)(x),$$
$$\exists\ g(x),\ com\ g(x) = 0,\ \forall x \in M,\ tal\ que\ (f + g)(x) = f(x) + g(x) = f(x) + 0 = f(x),$$
$$\exists\ -f(x),\ tal\ que\ (f + (-f))(x) = f(x) - f(x) = 0.$$

Agora vamos verificar as outras propriedades de módulo. Sejam $a, b \in A$, então:

$$a \cdot ((f + g)(x)) = a \cdot (f(x) + g(x)) = a \cdot f(x) + a \cdot g(x),$$
$$(a + b) \cdot f(x) = ((a + b) \cdot f)(x) = (a \cdot f + b \cdot f)(x) = a \cdot f(x) + b \cdot f(x),$$
$$(ab) \cdot f(x) = (ab \cdot f)(x) = a \cdot (b \cdot f)(x) = a \cdot (b \cdot f(x)),$$
$$1 \cdot f(x) = (1 \cdot f)(x) = f(x).$$

Portanto, $Hom(M, N)$ é um A-módulo. □

Os homomorfismos $u : M' \to M$ e $v : N \to N''$ induzem as aplicações

$$\overline{u}\colon Hom(M,N) \to Hom(M',N)$$

$$f \mapsto f \circ u$$

e

$$\overline{v}\colon Hom(M,N) \to Hom(M,N'')$$

$$f \mapsto v \circ f.$$

Proposição 2.6. *As aplicações $\overline{u}$ e $\overline{v}$ são homomorfismos de A-módulos.*

Demonstração. Seja $a \in M$, então para todo $x \in M$, temos que:

$$\overline{u}(f+g)(x) = (f+g)\circ u(x) = (f+g)(u(x)) = f(u(x)) + g(u(x)) = (f\circ u)(x) + (g\circ u)(x) = \overline{u}(f)(x) + \overline{u}(g)(x),$$
$$\overline{u}(a\cdot f)(x) = (a\cdot f)\circ u(x) = (a\cdot f)(u(x)) = a\cdot f(u(x)) = a\cdot(f\circ u)(x) = a\cdot\overline{u}(f)(x)$$

e

$$\overline{v}(f+g)(x) = v\circ(f+g)(x) = v(f+g)(x) = v(f)(x) + v(g)(x) = (v\circ f)(x) + (v\circ g)(x) = \overline{v}(f)(x) + \overline{v}(g)(x),$$
$$\overline{v}(a\cdot f)(x) = v\circ(a\cdot f)(x) = v(a\cdot f)(x) = a\cdot v(f)(x) = a\cdot(v\circ f)(x) = a\cdot\overline{v}(f)(x).$$

Portanto, $\overline{u}$ e $\overline{v}$ são homomorfismos de A-módulos. □

2.2 Submódulos e módulos quocientes

Definição 2.7. *Um submódulo M' de M é um subgrupo de M fechado em relação à multiplicação por elementos de A.*

Exemplo 2.8. *Se $f : M \to N$ é um homomorfismo de A-módulos, então o núcleo de f é o conjunto $ker(f) = \{x \in M : f(x) = 0\}$ e é um submódulo de M. De fato, se $x \in ker(f)$ e $a \in A$, então $f(ax) = a\cdot f(x) = a\cdot 0 = 0$, logo $ax \in ker(f)$. Além disso, se $x, y \in ker(f)$, então $f(x-y) = f(x) - f(y) = 0 - 0 = 0$, logo $x - y \in ker(f)$. Portanto, $ker(f)$ é um submódulo de M.*

Exemplo 2.9. *Se $f : M \to N$ é um homomorfismo de A-módulos, então a imagem de f é o conjunto $Im(f) = f(M)$ e é um submódulo de N. De fato, se $y \in Im(f)$ e $a \in A$, então $y = f(x)$, para algum $x \in M$, logo $ay = a\cdot f(x) = f(ax)$, portanto $ay \in Im(f)$. Além disso, se $x', y' \in Im(f)$, então $x' = f(x)$ e $y' = f(y)$, para alguns $x, y \in M$, logo $x' - y' = f(x) - f(y) = f(x-y)$, portanto $x' - y' \in Im(f)$. Portanto, $Im(f)$ é um submódulo de N.*

Definição 2.10. *O grupo abeliano M/M' herda a estrutura de A-módulo de M, com as operações definidas por*

$$(x + M') + (y + M') = (x + y) + M'$$

$$a(x + M') = ax + M'.$$

O A-módulo M/M' é chamado módulo quociente de M por M'.

Definição 2.11. *O conúcleo de f é definido por $Coker(f) = N/Im(f)$.*

Proposição 2.12. *Se M' é um submódulo de M tal que $M' \subseteq ker(f)$, então a aplicação*

$$\overline{f}\colon M/M' \to N$$

$$\overline{x} \mapsto f(x),$$

onde $\overline{x} = x + M'$, é um homomorfismo de A-módulos e é dito ser induzido do homomorfismo f. Além disso, o núcleo de $\overline{f}$ é $ker(f)/M'$.

Demonstração. A aplicação está bem definida, pois dados $\overline{x}, \overline{y} \in M/M'$, se $\overline{x} = \overline{y}$, então $x - y \in M'$. Como $M' \subseteq ker(f)$, então $f(x - y) = 0$, logo $f(x) - f(y) = 0$, o que implica $\overline{f}(\overline{x}) - \overline{f}(\overline{y}) = 0$, portanto $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$. A aplicação é um homomorfismo, pois dados $\overline{x}, \overline{y} \in M/M'$ e $a \in A$, temos que $\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y})$ e $\overline{f}(a\overline{x}) = f(ax) = a \cdot f(x) = a \cdot \overline{f}(\overline{x})$. Por fim, temos que $ker(\overline{f}) = \{\overline{x} : f(x) = 0\} = \{\overline{x} : x \in ker(f)\} = ker(f)/M'$. □

Observação 2.13. *Em particular, tomando $M' = ker(f)$, temos que $ker(\overline{f}) = ker(f)/M' = ker(f)/ker(f) = \overline{0}$, e então $\overline{f}$ é injetor e portanto $\overline{f} : M/ker(f) \to Im(\overline{f})$ é um isomorfismo de A-módulos.*

2.3 Operações com submódulos

Definição 2.14. *Seja M um A-módulo e seja $(M_i)_{i \in I}$ uma família de submódulos de M, definimos a soma $\sum_{i \in I} M_i$ como o conjunto de todas as somas finitas $\sum x_i$, onde $x_i \in M_i$, para todo $i \in I$.*

Definição 2.15. *Seja M um A-módulo e seja $(M_i)_{i \in I}$ uma família de submódulos de M, definimos a interseção $\bigcap_{i \in I} M_i = \{x \in M$, com $x \in M_i$, para todo $i \in I\}$.*

Proposição 2.16. *A soma $\sum_{i \in I} M_i$ é o menor submódulo de M contendo todos os M_i e a interseção de qualquer família $(M_i)_{i \in I}$ de submódulos de M é um submódulo de M.*

Demonstração. A demonstração é análoga a feita para ideais nas Proposições 1.58 e 1.60. □

Observação 2.17. *Diferente do caso dos ideais, não definimos o produto de submódulos.*

Definição 2.18. *Sejam N, P submódulos de M, definimos o quociente $(N : P)$ como o conjunto de todos os elementos $a \in A$ tais que $aP \subseteq N$.*

Proposição 2.19. *O quociente $(N : P)$ é um ideal de A.*

Demonstração. Sejam $x, y \in (N : P)$. Então $xP \subseteq N$ e $yP \subseteq N$. Seja $p' \in P$. Temos que $(x-y)p' = xp' - yp' \in N$, pois N é submódulo e portanto subgrupo aditivo. Como p' é arbitrário, temos que $(x-y)P \subseteq N$. Portanto, $x - y \in (N : P)$. Agora, sejam $x \in (N : P)$, $a \in A$ e $p' \in P$. Temos que $ax \in A(N : P)$ e $axp' = (xp')a \in N$, pois N é submódulo e portanto fechado em relação a multiplicação por elementos de A. Como p' é arbitrário, temos que $axP \subseteq N$, logo $ax \in (N : P)$. Portanto, $A(N : P) \subseteq (N : P)$. Assim, temos que $(N : P)$ é ideal de A. □

Definição 2.20. *O quociente* $(0 : M)$ *é o conjunto de todos os elementos* $a \in A$ *tais que* $aM = 0$ *e este ideal é chamado de anulador de* M *e denotado por* $Ann(M)$.

Se $I \subseteq Ann(M)$, podemos considerar M como um A/I-módulo, como a seguir: se $\overline{a} \in A/I$ é representado por $a \in A$, definimos $\overline{a}m$ por am, com $m \in M$. Este processo é independente da escolha do representante a de $\overline{a}$, uma vez que $IM = 0$. De fato, seja $\overline{a} = a + I = b + I = \overline{b}$. Então, $a - b \in I \subseteq Ann(M)$ e $(a-b) \cdot m = 0$, para qualquer $m \in M$. Logo $am - bm = 0 \Rightarrow am = bm$.

Proposição 2.21. *São válidas as seguintes igualdades:*

i) $Ann(M + N) = Ann(M) \cap Ann(N)$;

ii) $(N : P) = Ann((N + P)/N)$.

Demonstração. i) Seja $x \in Ann(M + N)$, então $x(m + n) = 0$, para todo $m \in M$ e $n \in N$. Se $m = 0$, então $xn = 0$, logo $x \in Ann(N)$. Se $n = 0$, então $xm = 0$, logo $x \in Ann(M)$. Portanto $x \in Ann(M) \cap Ann(N)$. Por outro lado, seja $y \in Ann(M) \cap Ann(N)$, então $ym = yn = 0$, para todo $m \in M$ e $n \in N$. Logo, $ym + yn = y(m + n) = 0$, com $m + n \in M + N$, e então $y \in Ann(M + N)$. Portanto, $Ann(M + N) = Ann(M) \cap Ann(N)$.

ii) Seja $x \in (N : P)$, então $xP \subseteq N$. Como $P \subseteq P + N$, temos que $xP \subseteq x(P + N) \subseteq N$. Logo $x \cdot \dfrac{(P+N)}{N} = 0$, e então $x \in Ann((N + P)/N)$. Por outro lado, se $x \in Ann((N + P)/N)$, então $x \cdot \dfrac{(P+N)}{N} = 0$. Logo, $x(N + P) \subseteq N$, ou seja, $xN + xP \subseteq N$. Então $xP \subseteq N$, logo $x \in (N : P)$. Portanto, $(N : P) = Ann((N + P)/N)$.

□

2.4 Sequências exatas

Definição 2.22. *Uma sequência de A-módulos e A-homomorfismos*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

é dita ser exata em M_i se $Im(f_i) = ker(f_{i+1})$. A sequência é chamada de sequência exata se é exata em cada M_i.

Proposição 2.23. *i) A sequência $0 \xrightarrow{f} M' \xrightarrow{f'} M$ é exata se, e somente se, f' é injetora.*

ii) A sequência $M \xrightarrow{g} M'' \xrightarrow{g'} 0$ é exata se, e somente se, g é sobrejetora.

Demonstração. i) A sequência é exata se, e somente se, $Im(f) = ker(f')$, mas como f é um homomorfismo, temos que $Im(f) = 0_{M'}$, logo a sequência é exata se, somente se, $0_{M'} = Im(f) = ker(f')$. Mas $ker(f') = 0_{M'}$ se, e somente se, f' é injetora. Portanto, a seqûencia é exata se, e somente se, f' é injetora.

ii) A sequência é exata se, e somente se, $Im(g) = ker(g')$, mas como $Im(g') = 0$, temos que $ker(g') = M''$, logo a sequência é exata se, somente se, $Im(g) = M''$, o que ocorre se, e somente se, g for sobrejetora. Portanto, a seqûencia é exata se, e somente se, g é sobrejetora.

□

Lema 2.24 (Lema da Serpente)**.** *Seja*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' \longrightarrow 0 \\ & & f' \downarrow & & f \downarrow & & f'' \downarrow \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' \longrightarrow 0 \end{array}$$

um diagrama comutativo de A-módulos e homomorfismos, cujas linhas são sequências exatas. Então existe uma sequência exata

$$0 \longrightarrow ker(f') \xrightarrow{\overline{u}} ker(f) \xrightarrow{\overline{v}} ker(f'') \xrightarrow{d} Coker(f') \xrightarrow{\overline{u'}} Coker(f) \xrightarrow{\overline{v'}} Coker(f'') \longrightarrow 0$$

onde $\overline{u}$ e $\overline{v}$ são as restrições de u e v respectivamente e $\overline{u'}$ e $\overline{v'}$ são induzidas por u' e v' respectivamente.

Demonstração. Primeiramente, vamos definir o homomorfismo de fronteira d. Seja $x \in ker(f'')$. Como v é sobrejetora, temos que $x = v(z)$, para algum $z \in M$. Assim, $v'(f(z)) = f''(v(z)) = f''(x) = 0$, logo $f(z) \in ker(v') = Im(u')$. Seja $f(z) = u'(y)$, para algum $y \in N'$. Assim, temos o homomorfismo

$$\begin{aligned} d\colon ker(f'') &\to Coker(f') = N'/Im(f') \\ x &\mapsto y + Im(f'). \end{aligned}$$

Do traçado dado por este homomorfismo d, originou-se o nome de Lema da Serpente, conforme a Figura 2.1.

Devido ao tamanho extenso da demonstração do Lema da Serpente, a prova de que os homomorfismos $\overline{u}, \overline{v}, d, \overline{u'}$ e $\overline{v'}$ estão bem definidos não será feita neste trabalho e pode ser encontrada nas referências [3] e [2]. Agora, vamos mostrar que a sequência é exata em cada um dos A-módulos.

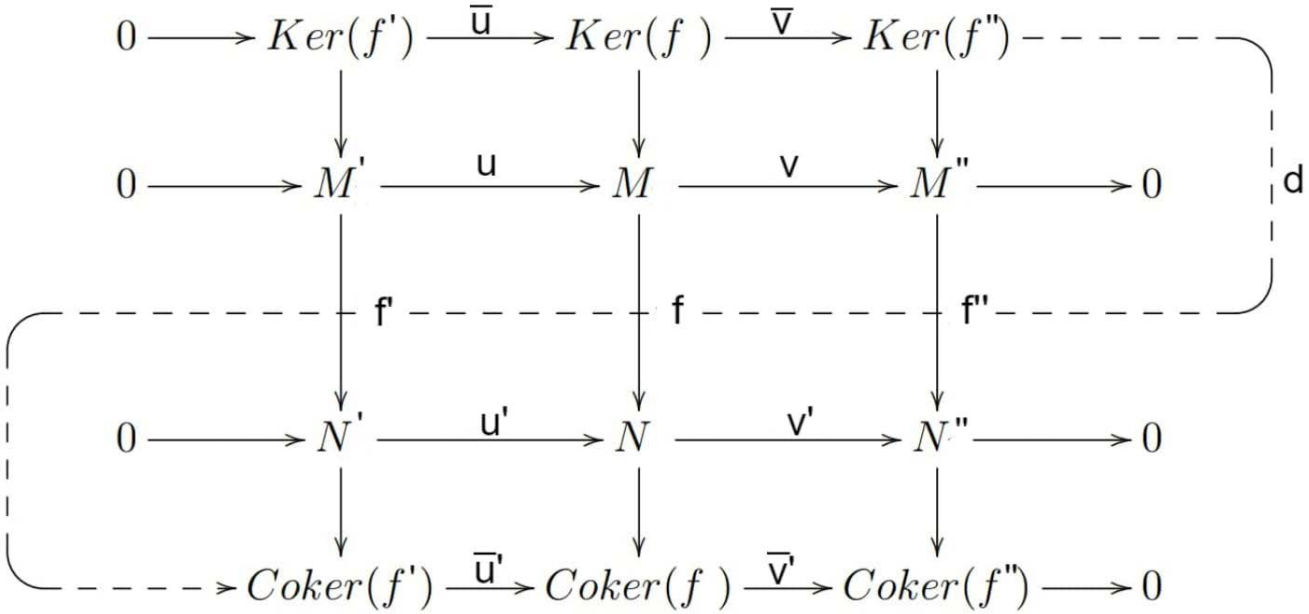

Figura 2.1: Diagrama do Lema da Serpente

i) A sequência é exata em $ker(f')$. De fato, como u é injetor e $\overline{u}$ é a restrição de u, temos que $\overline{u}$ é injetor. Logo, pelo item i) da Proposição 2.23, temos que a sequência é exata em $ker(f')$.

ii) A sequência é exata em $ker(f)$, isto é, $Im(\overline{u}) = ker(\overline{v})$. De fato, como $\overline{u}$ e $\overline{v}$ são as restrições de u e v respectivamente, temos que $\overline{v} \circ \overline{u} = (v \circ u)|_{ker(f')}$ e por hipótese $Im(u) = ker(v)$, logo $v \circ u \equiv 0$, portanto $\overline{v} \circ \overline{u} = 0$, ou seja, $Im(\overline{u}) \subseteq ker(\overline{v})$.

Agora, seja $x \in ker(\overline{v})$, então $x \in ker(f)$. Assim, $\overline{v}(x) = f(x) = 0$, e como $\overline{v}$ é a restrição v, segue que $v(x) = 0$. Por hipótese, temos que $ker(v) = Im(u)$, e como $v(x) = 0$, temos que $x \in ker(v)$, logo $x \in Im(u)$, isto é, $x = u(y)$, para algum $y \in M'$. Mas $0 = f(x) = f(u(y)) = u'(f'(y))$, e como u' é injetor, então $f'(y) = 0$. Logo $y \in ker(f')$ e como $\overline{u}$ é restrição de u, então $\overline{u}(y) = u(y) = x$. Portanto, $x \in Im(\overline{u})$, logo $ker(\overline{v}) \subseteq Im(\overline{u})$.

Assim, concluímos que $Im(\overline{u}) = ker(\overline{v})$, e portanto a sequência é exata em $ker(f)$ como queríamos provar.

iii) A sequência é exata em $ker(f'')$, isto é, $Im(\overline{v}) = ker(d)$. De fato, seja $y \in Im(\overline{v})$, então existe $x \in ker(f)$, tal que $\overline{v}(x) = y \in ker(f'')$. Temos que $d(y) = 0 + Im(f')$, pois $u'(0) = f(x) = 0$, com $v(x) = \overline{v}(x) = y$. Logo $y \in ker(d)$ e portanto, $Im(\overline{v}) \subseteq ker(d)$.

Por outro lado, seja $y \in ker(d)$, então $d(y) = z + Im(f')$, com $u'(z) = f(x), v(x) = y$ e $z \in Im(f')$, então existe $w \in M$, tal que $f'(w) = z$. Assim, $u'(z) = u'(f'(w)) = f(u(w))$. Temos que

$v(u(w)) = 0$ pois por hipótese $Im(u) = ker(v)$, assim $v(x-u(w)) = v(x)-v(u(w)) = v(x)-0 = v(x)$, então temos que $x-u(w)$ satisfaz as condições de d. Como $f(x-u(w)) = f(x)-f(u(w)) = u'(z)-u'(z) = 0$, temos que $x-u(w) \in ker(f)$. Assim, tomamos $y = \overline{v}(x-u(w))$, logo $u \in Im(\overline{v})$, então $ker(d) \subseteq Im(\overline{v})$.

Portanto, $Im(\overline{v}) = ker(d)$ e a sequência é exata em $ker(f'')$, como queríamos provar.

iv) A sequência é exata em $Coker(f')$, isto é, $Im(d) = ker(\overline{u'})$. De fato, seja $\overline{y} \in ker(\overline{u'})$, então $\overline{u'}(\overline{y}) = \overline{u'}(y + Im(f')) = u'(y) + Im(f) = Im(f)$ se, e somente se, $u'(y) = f(x)$, para algum $x \in M$. Tomando $z = v(x)$, temos que $d(z) = \overline{y}$, logo $\overline{y} \in Im(d)$, portanto $ker(\overline{u'}) \subseteq Im(d)$.

Agora, seja $x \in ker(f'')$, como v é sobrejetor, temos que $x = v(z)$, para algum $z \in M$, e pela definição de d temos que $d(x) = y + Im(f')$, onde y é tal que $u'(y) = f(z) \in Im(f)$ e então $\overline{u'} \circ d(x) = \overline{u'}(y + Im(f')) = u'(y) + Im(f)$. Logo $\overline{u'}(d(x)) = Im(f)$, pois $u'(y) \in Im(f)$. Daí segue que $d(x) \in ker(\overline{u'})$ e portanto $Im(d) \subseteq ker(\overline{u'})$.

Dessa forma, temos que $Im(d) = ker(\overline{u'})$ e portanto a sequência é exata em $Coker(f')$, como queríamos provar.

v) A sequência é exata em $Coker(f)$, isto é, $Im(\overline{u'}) = ker(\overline{v'})$. De fato, seja $x \in M'$ e $\overline{x} = x + Im(f') \in Coker(f)$, então $\overline{v'} \circ \overline{u'}(\overline{x}) = \overline{v'}(u'(x) + Im(f)) = v'(u'(x)) + Im(f'')$. Como $Im(u') = ker(v')$, temos que $v' \circ u' \equiv 0$, logo $\overline{v'} \circ \overline{u'}(\overline{x}) = Im(f'')$. Portanto $Im(\overline{u'}) \subseteq ker(\overline{v'})$.

Por outro lado, tomando $\overline{y} \in ker(\overline{v'})$, temos que $\overline{v'}(\overline{y}) = \overline{v'}(y+Im(f)) = v'(y)+Im(f'') = Im(f'')$ se, e somente se, $v'(y) \in Im(f'')$. Assim, existe $z \in M''$, tal que $f''(z) = v'(y)$. Como v é sobrejetor, existe $x \in M$, tal que $v(x) = z$. Fazendo $v'(y - f(x)) = v'(y) - v'(f(x)) = v'(y) - f''(v(x)) = v'(y)-f''(z) = 0$, obtemos $y-f(x) \in ker(v') = Im(u')$. Logo, existe $w \in N'$, tal que $u'(w) = y - f(x)$. Portanto, $\overline{u'}(\overline{w}) = \overline{u'}(w + Im(f')) = u'(w) + Im(f) = y - f(x) + Im(f) = \overline{y}$. Logo, $ker(\overline{v'}) \subseteq Im(\overline{u'})$.

Portanto, $Im(\overline{u'}) = ker(\overline{v'})$ e a sequência é exata em $Coker(f)$, como queríamos provar.

vi) A sequência é exata em $Coker(f'')$. De fato, como v' é sobrejetor e $\overline{v'}$ é restrição de v', temos que $\overline{v'}$ é sobrejetor. Logo, pelo item $ii)$ da Proposição 2.23, temos que a sequência é exata em $ker(f')$.

Dessa forma, provamos que a sequência é exata em cada um de seus A-módulos e portanto é uma seqüência exata. □

Capítulo 3

Anéis de Frações e Módulos de Frações

Neste capítulo, iremos apresentar os conceitos, propriedades e resultados básicos sobre anéis de frações e módulos de frações.

O procedimento através do qual obtemos o corpo $\mathbb{Q}$ a partir do anel $\mathbb{Z}$ pode ser estendido a um domínio de integridade A, produzindo o corpo de frações de A. A construção consiste em tomar todos os pares ordenados (a, s), com $a, s \in A$ e $s \neq 0$, e definir uma relação de equivalência entre tais pares da seguinte forma: para todos $(a, s), (b, t)$, com $a, b, s, t \in A$, $s \neq 0$ e $t \neq 0$, temos que

$$(a, s) \equiv (b, t) \Leftrightarrow at - bs = 0.$$

Observação 3.1. *Notemos que este processo só é válido em domínios de integridade, pois a verificação de que esta relação é transitiva envolve cancelamento de termos, isto é, o fato de que A não possui divisores de zeros não nulos. De fato, sejam $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$, onde $a, b, c, s, t, u \in A$, $s \neq 0$, $t \neq 0$ e $u \neq 0$. Queremos mostrar que $(a, s) \equiv (c, u)$. Temos que $(a, s) \equiv (b, t)$ se, e somente se, $at - bs = 0$ e que $(b, t) \equiv (c, u)$ se, e somente se, $bu - ct = 0$. Assim, temos o sistema*

$$\begin{cases} at - bs = 0 & (\times\ u) \\ bu - ct = 0 & (\times\ s) \end{cases} \implies \begin{cases} atu - bsu = 0 \\ bus - cts = 0 \end{cases}$$

Somando as duas equações temos que

$$atu - bsu + bsu - cts = 0 \implies atu - cts = 0 \implies (au - cs)t = 0.$$

Como A é domínio de integridade, temos que $au - cs = 0$ ou $t = 0$. Mas por hipótese $t \neq 0$, logo $au - cs = 0$, ou seja, $(a, s) \equiv (c, u)$, como queríamos provar.

Apesar deste processo, como definido anteriormente, ser válido apenas em domínios de integridade, veremos que é possível, mudando a relação de equivalência, generalizá-lo para qualquer anel A, produzindo o anel de frações de A.

Definição 3.2. *Seja A um anel. Um sistema multiplicativo fechado de A é um subconjunto S de A tal que $1 \in S$ e S é fechado em relação à multiplicação.*

Definimos uma relação $\equiv$ em $A \times S$, da seguinte forma: para todos $(a, s), (b, t) \in A \times S$, temos

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

Proposição 3.3. *A relação definida acima é uma relação de equivalência.*

Demonstração. i) A relação é reflexiva, pois para todo par $(a, s) \in A \times S$, temos que $(as - as)u = 0$, para todo $u \in S$, logo $(a, s) \equiv (a, s)$.

ii) A relação é simétrica, pois para todos os pares $(a, s), (b, t) \in A \times S$, temos que $(a, s) \equiv (b, t)$, o que implica $(at - bs)u = 0$, para algum $u \in S$, logo $(bs - at) \cdot (-u) = 0$ e portanto $(b, t) \equiv (a, s)$.

iii) A relação é transitiva, pois para todos os pares $(a, s), (b, t), (c, u) \in A \times S$, supondo que $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$, temos que existem $v, w \in S$ tais que $(at - bs)v = 0$ e $(bu - ct)w = 0$. Assim, temos o sistema

$$\begin{cases} (at - bs)v = 0 \\ (bu - ct)w = 0 \end{cases} \implies \begin{cases} atv - bsv = 0 \quad (\times\ uw) \\ buw - ctw = 0 \quad (\times\ sv) \end{cases} \implies \begin{cases} atvuw - bsvuw = 0 \\ buwsv - ctwsv = 0 \end{cases}$$

Somando as duas equações temos que

$$atvuw - bsvuw + buwsv - ctwsv = 0 \implies atvuw - ctwsv = 0 \implies (au - cs)tvw = 0.$$

Como $t, v, w \in S$ e S é multiplicativamente fechado, temos que $tvw \in S$, logo $(a, s) \equiv (c, u)$, como queríamos provar.

□

Vamos denotar por a/s a classe de equivalência de $(a, s) \in A \times S$, e por $S^{-1}A$ o conjunto destas classes de equivalência. Colocamos uma estrutura de anel em $S^{-1}A$ definindo a adição e multiplicação destas "frações" a/s da mesma forma que na álgebra elementar, ou seja, dados $(a, s), (b, t) \in A \times S$, temos

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad e \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Proposição 3.4. *As operações definidas acima independem da escolha dos representantes $(a, s), (b, t) \in A \times S$ e portanto estão bem definidas.*

Demonstração. Sejam $a/s = a'/s'$ e $b/t = b'/t'$, onde $(a, s), (a', s'), (b, t), (b', t') \in A \times S$. Temos que

$$\begin{cases} (as' - a's)u = 0 \quad (\times\ vtt') \\ (bt' - b't)v = 0 \quad (\times\ uss') \end{cases} \implies \begin{cases} as'uvtt' - a'suvtt' = 0 \\ bt'vuss' - b'tvuss' = 0 \end{cases}$$

Somando as duas equações temos que

$$(as'tt' + bt'ss')uv - (bt'ss' + b'tss')uv = 0 \implies [(at + bs)t's' - (a't' + b's')st]uv = 0.$$

Portanto

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'}.$$

Além disso, temos que

$$\begin{cases} (as' - a's)u = 0 \quad (\times\ bt'v) \\ (bt' - b't)v = 0 \quad (\times\ a'su) \end{cases} \implies \begin{cases} as'bt'uv - a'sbt'uv = 0 \\ bt'a'svu - b'ta'svu = 0 \end{cases}$$

Somando as duas equações temos que

$$(as'bt' - b'ta's)uv = 0 \implies (abs't' - a'b'st)uv = 0.$$

Portanto

$$\frac{ab}{st} = \frac{a'b'}{s't'}.$$

□

Proposição 3.5. *$S^{-1}A$ satisfaz as propriedades de um anel comutativo com unidade.*

Demonstração. Sejam $(a, s), (b, t), (c, u) \in A \times S$. Temos que:

A1: A adição é associativa:

$$\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} = \frac{at + bs}{st} + \frac{c}{u} = \frac{atu + bsu + cst}{stu} = \frac{a}{s} + \frac{bu + ct}{tu} = \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right).$$

A2: Existe um elemento neutro com respeito a adição:

$$\frac{0}{1} + \frac{a}{s} = \frac{0 \cdot s + a \cdot 1}{1 \cdot s} = \frac{0 + a}{s} = \frac{a}{s}$$

A3: Todo elemento de A possui um inverso com respeito a adição:

$$\frac{a}{s} + \frac{-a}{s} = \frac{as - as}{s^2} = \frac{0}{s^2} = \frac{0}{1},\ \textit{pois}\ (0 \cdot 1 - s^2 \cdot 0)u = 0, \forall u \in S.$$

A4: A adição é comutativa:

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

M1: A multiplicação é associativa:

$$\left(\frac{a}{s} \cdot \frac{b}{t}\right) \cdot \frac{c}{u} = \frac{ab}{st} \cdot \frac{c}{u} = \frac{abc}{stu} = \frac{a}{s} \cdot \frac{bc}{tu} = \frac{a}{s} \cdot \left(\frac{b}{t} \cdot \frac{c}{u}\right).$$

M2: Existe um elemento neutro com respeito a multiplicação:

$$\frac{a}{s}\cdot\frac{1}{1}=\frac{a\cdot 1}{s\cdot 1}=\frac{a}{s}$$

M3: A multiplicação é comutativa:

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

AM: A adição é ditributiva em relação à multiplicação:

$$\frac{a}{s}\cdot\left(\frac{b}{t}+\frac{c}{u}\right)=\frac{a}{s}\cdot\left(\frac{bu+ct}{tu}\right)=\frac{abu+act}{stu}=\frac{abu}{stu}+\frac{act}{stu}=\frac{ab}{st}+\frac{ac}{su}=\frac{a}{s}\cdot\frac{b}{t}+\frac{a}{s}\cdot\frac{c}{u}.$$

□

Proposição 3.6. *A função $f : A \to S^{-1}A$, definida por $f(x) = \frac{x}{1}$, para todo $x \in A$, é um homomorfismos de anéis.*

Demonstração. Sejam $x, y \in A$. Então

$$f(x+y)=\frac{x+y}{1}=\frac{x\cdot 1+y\cdot 1}{1\cdot 1}=\frac{x}{1}+\frac{y}{1}=f(x)+f(y).$$

$$f(x\cdot y)=\frac{x\cdot y}{1}=\frac{x\cdot y}{1\cdot 1}=\frac{x}{1}\cdot\frac{y}{1}=f(x)\cdot f(y).$$

□

Exemplo 3.7. *O homomorfismo de anéis acima, em geral, não é injetor. De fato, seja $A = \mathbb{Z}_6$ e $S = \mathbb{Z}_6 - \{\overline{0}, \overline{3}\}$. Temos que S é um conjunto multiplicativamente fechado e que $\overline{0} \neq \overline{3}$, mas $f(\overline{0}) = f(\overline{3})$. De fato,*

$$\frac{\overline{3}}{\overline{1}}=\frac{\overline{0}}{\overline{1}}\Leftrightarrow(\overline{3}\cdot\overline{1}-\overline{1}\cdot\overline{0})u=\overline{0},\ \textit{para algum } u\in S\Leftrightarrow\overline{3}\cdot u=\overline{0}.$$

Tomando $u = \overline{2} \in S$, temos que $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ em S. Portanto, o homomorfismo f não é injetor.

Definição 3.8. *O anel $S^{-1}A$ é chamado de anel de frações de A em relação a S. Em particular, quando A é um domínio de integridade e $S = A - \{0\}$, então $S^{-1}A$ é chamado corpo de frações de A.*

Proposição 3.9. *Seja $f : A \to S^{-1}A$, o homomorfismo definido por $f(x) = \frac{x}{1}$ e seja $g : A \to B$ um homomorfismo de anéis tal que $g(s)$ é uma unidade em B para todo $s \in S$. Então existe um único homomorfismo de anéis $h : S^{-1}A \to B$ tal que $g = h \circ f$.*

Demonstração. i) Unicidade: Se h satisfaz as condições, então $h(a/1) = h(f(a)) = g(a)$, para todo $a \in A$. Para $s \in S$, temos que $s \in A$ e $1 \in S$, então se $s \in S$, temos que $h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$ e, portanto temos que $h(a/s) = h(a/1) \cdot h(1/s) = g(a)g(s)^{-1}$, implicando que h é unicamente determinado por g.

ii) Existência: Para $(a/s) \in S^{-1}A$, seja $h(a/s) = g(a)g(s)^{-1}$. Então h é um homomorfismo de anéis que está bem definido. De fato, sejam $a/s, a'/s' \in S^{-1}A$, tais que $a/s = a'/s'$, então existe $t \in S$ tal que $(as' - a's)t = 0$, logo

$$[g(a)g(s') - g(a')g(s)]g(t) = 0. \tag{3.1}$$

Como $g(t)$ é unidade em B, segue que $g(a)g(s)^{-1} = g(a')g(s')^{-1}$.

□

Proposição 3.10. *O anel $S^{-1}A$ e o homomorfismo $f : A \to S^{-1}A$ satisfazem as seguintes propriedades:*

i) Se $s \in S$, então $f(s)$ é uma unidade em $S^{-1}A$.

ii) Se $f(a) = 0$, então $as = 0$, para algum $s \in S$.

iii) Todo elemento de $S^{-1}A$ é da forma $f(a)f(s)^{-1}$, para algum $a \in A$ e algum $s \in S$.

Demonstração. i) Como $f(s) = s/1$ e $S^{-1}A = \{a/s : a \in A, s \in S\}$, em particular, $1/s \in S^{-1}A$ e $(1/s)(s/1) = 1$.

ii) Como $f(a) = 0$, então $a/1 = 0/1$, logo $(a \cdot 1 - 1 \cdot 0)s = 0$, portanto $as = 0$ para algum $s \in S$.

iii) Se $x \in S^{-1}A$, então $x = a/s = (a/1) \cdot (1/s) = f(a) \cdot f(s)^{-1}$.

□

Por outro lado, estas três condições determinam um isomorfismo de $S^{-1}A$ em B. Mais precisamente, temos o seguinte resultado:

Proposição 3.11. *Se $g : A \to B$ é um homomorfismo de anéis tal que:*

i) Se $s \in S$, então $g(s)$ é uma unidade em B.

ii) Se $g(a) = 0$, então $as = 0$, para algum $s \in S$.

iii) Todo elemento de B é da forma $g(a)g(s)^{-1}$, para algum $a \in A$ e algum $s \in S$.

Então, existe um único isomorfismo $h : S^{-1}A \to B$, tal que $g = h \circ f$.

Demonstração. Pela Proposição 3.9, temos que mostrar que $h : S^{-1}A \to B$, definida por $h(a/s) = g(a)g(s)^{-1}$ é um isomorfismo. Note que esta definição para h utiliza a condição (i). Pelo item (iii), h é sobrejetora. Para mostrar que h é injetora, vamos analisar o seu núcleo: se $h(a/s) = 0$, então $g(a) = 0$, e assim, pelo item (ii), temos que $at = 0$, para algum $t \in S$. Portanto, $(a, s) \equiv (0, 1)$, isto é, $a/s = 0$ em $S^{-1}A$. □

A construção de $S^{-1}A$ pode ser feita com um A-módulo M ao invés de um anel A. Definimos a relação $\equiv$ em $M \times S$ da seguinte maneira: sejam $(m,s),(m',s') \in M \times S$, temos

$$(m,s) \equiv (m',s') \Leftrightarrow \exists t \in S, \text{ tal que } t(sm' - s'm) = 0.$$

Observação 3.12. *A relação definida acima é uma relação de equivalência e a demonstração é a mesma da feita para anéis na Proposição 3.3.*

Notação. Denotemos por m/s a classe de equivalência do par (m,s) e por $S^{-1}M$ o conjunto de tais frações.

Proposição 3.13. *$S^{-1}M$ é um $S^{-1}A$-módulo com as definições usuais de adição e multiplicação por escalar.*

Demonstração. Sejam m/s e $n/t \in S^{-1}M$. Vamos verificar que $S^{-1}M$ é um grupo abeliano aditivo. $S^{-1}M$ é fechado pela operação:

$$\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st} \in S^{-1}M,$$

uma vez que, como $mt \in M, ns \in M$ e M é um grupo aditivo, então $mt+ns \in M$, e como $s \in S, t \in S$ e S é multiplicativamente fechado, então $st \in S$.

A prova que existe um elemento neutro aditivo, um elemento inverso aditivo e que a adição é associativa é a mesma feita para $S^{-1}A$ na Proposição 3.5.

Agora vamos verificar as outras propriedades de módulo. Sejam a/b e $c/d \in S^{-1}A$. Então:

i) $\dfrac{a}{b} \cdot \left(\dfrac{m}{s} + \dfrac{n}{t}\right) = \dfrac{a}{b} \cdot \dfrac{mt+ns}{st} = \dfrac{amt+ans}{bst} = \dfrac{amt}{bst} + \dfrac{ans}{bst} = \dfrac{a}{b} \cdot \dfrac{m}{s} + \dfrac{a}{b} \cdot \dfrac{n}{t}$;

ii) $\left(\dfrac{a}{b} + \dfrac{c}{d}\right) \cdot \dfrac{m}{s} = \dfrac{ad+cb}{bd} \cdot \dfrac{m}{s} = \dfrac{adm+cbm}{bds} = \dfrac{adm}{bds} + \dfrac{cbm}{bds} = \dfrac{a}{b} \cdot \dfrac{m}{s} + \dfrac{c}{d} \cdot \dfrac{m}{s}$;

iii) $\left(\dfrac{a}{b} \cdot \dfrac{c}{d}\right) \cdot \dfrac{m}{s} = \dfrac{ac}{bd} \cdot \dfrac{m}{s} = \dfrac{acm}{bds} = \dfrac{a}{b} \cdot \dfrac{cm}{ds} = \dfrac{a}{b} \cdot \left(\dfrac{c}{d} \cdot \dfrac{m}{s}\right)$;

iv) $\dfrac{1}{1} \cdot \dfrac{m}{s} = \dfrac{1 \cdot m}{1 \cdot s} = \dfrac{m}{s}$.

Portanto, $S^{-1}M$ é um $S^{-1}A$-módulo, como queríamos provar. □

Seja $u : M \to N$ um homomorfismo de A-módulos. Então u origina um homomorfismo de $S^{-1}A$-módulos $S^{-1}u : S^{-1}M \to S^{-1}N$, que leva m/s em $u(m)/s$. Assim, se $M' \xrightarrow{u} M$ e $M \xrightarrow{v} M''$ temos que $S^{-1}(v \circ u) = S^{-1}(v) \circ S^{-1}(u)$.

Proposição 3.14. *A operação S^{-1} é exata, isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata em M, então $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é exata em $S^{-1}M$.*

Demonstração. Temos que $g \circ f = 0$, então $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$, logo $Im(S^{-1}f) \subseteq ker(S^{-1}g)$. Para provar a inclusão contrária, seja $m/s \in ker(S^{-1}g)$, então $g(m)/s = 0$ em $S^{-1}M''$. Assim, existe $t \in S$ tal que $tg(m) = 0$ em M''. Mas $tg(m) = g(tm)$, pois g é um homomorfismo de A-módulos, logo $tm \in ker(g) = Im(f)$, assim $tm = f(m')$, para algum $m' \in M'$. Dessa forma, em $S^{-1}M$, temos que $m/s = f(m')/st = (S^{-1}f)(m'/st) \in Im(S^{-1}f)$. Portanto $ker(S^{-1}g) \subseteq Im(S^{-1}f)$. □

Em particular, segue deste resultado que se M' é um submódulo de M, então a função $S^{-1}M' \to S^{-1}M$ é injetora, e portanto $S^{-1}M'$ pode ser considerado como um submódulo de $S^{-1}M$. Com isso, temos o seguinte corolário:

Corolário 3.15. *Se N e P são submódulos de um A-módulo M, então:*

i) $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$.

ii) $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$.

iii) os $S^{-1}A$-módulos $S^{-1}(M/N)$ e $S^{-1}(M)/S^{-1}(N)$ são isomorfos.

Demonstração. i) Seja $\frac{n+p}{s} \in S^{-1}(N + P)$, com $n \in N$ e $p \in P$. Temos que $\frac{n+p}{s} = \frac{ns+ps}{s^2} = \frac{n}{s} + \frac{p}{s} \in S^{-1}N + S^{-1}P$. Logo $S^{-1}(N + P) \subseteq S^{-1}(N) + S^{-1}(P)$. Por outro lado, seja $\frac{n'}{s'} + \frac{p'}{t'} \in S^{-1}(N) + S^{-1}(P)$. Temos que $\frac{n'}{s'} + \frac{p'}{t'} = \frac{t'n' + s'p'}{s't'}$. Mas $s't' \in S$, $t'n' \in N$ e $s'p' \in P$, logo $\frac{t'n' + s'p'}{s't'} \in S^{-1}(N + P)$ e então $S^{-1}(N) + S^{-1}(P) \subseteq S^{-1}(N + P)$. Portanto, vale a igualdade.

ii) Seja $y/s = z/t \in S^{-1}N \cap S^{-1}P$, com $y \in N; z \in P; s, t \in S$, então $u(ty - sz) = 0$, para algum $u \in S$. Logo $w = uty = usz \in N \cap P$ e $y/s = z/t = zus/tus = w/stu \in S^{-1}(N \cap P)$. Consequentemente, $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$. A inclusão inversa se dá pois se $x \in S^{-1}(N \cap P)$, então $x = a/s$, com $a \in N$ e $a \in P$.

iii) Aplicando S^{-1} à sequência exata $0 \longrightarrow N \xrightarrow{\psi} M \xrightarrow{\phi} M/N \longrightarrow 0$, temos que a sequência $0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}(M/N) \longrightarrow 0$ é exata pela Proposição 3.14. Como $S^{-1}\phi$ é um homomorfismo sobrejetor, e $ker(S^{-1}\phi) = S^{-1}N$, temos pela Observação 2.13 que $S^{-1}\left(\frac{M}{N}\right) \simeq \frac{S^{-1}M}{S^{-1}N}$.

□

No que segue, consideramos o homomorfismo de anéis $f : A \to S^{-1}A$ definido na Proposição 3.6.

Proposição 3.16. *Seja I um ideal em A, então sua extensão I^e em $S^{-1}A$ é $S^{-1}I$.*

Demonstração. Seja $a/s \in I^e$, então

$$\begin{aligned} a/s &= \sum y_i f(x_i),\ com\ x_i \in I\ e\ y_i \in S^{-1}A \\ &= \sum b_i/t_i \cdot x_i/1,\ com\ b_i \in A\ e\ t_i \in S \\ &= \sum b_i x_i/t_i \\ &= \frac{b_1 x_1 s_2 s_3 \cdots + b_2 x_2 s_1 s_3 \cdots + \cdots}{s_1 s_2 s_3 \cdots}. \end{aligned}$$

Como cada $x_i \in I$, então temos que $b_1 x_1 s_2 s_3 \cdots + b_2 x_2 s_1 s_3 \cdots + \cdots \in I$, e como cada $s_i \in S$, então $s_1 s_2 s_3 \cdots \in S$. Logo $a/s \in S^{-1}I$ e portanto $I^e \subseteq S^{-1}I$. Por outro lado, seja $b/t \in S^{-1}I$, então $b \in I$ e $t \in S$. Note que $b/t = b/1 \cdot 1/t = f(b) \cdot 1/t$. Como $f(b) \in f(I)$ e $1/t \in S^{-1}A$, segue que $b/t \in f(I)S^{-1}A = I^e$ e portanto $S^{-1}I \subseteq I^e$. Como as duas inclusões são verdadeiras, então $I^e = S^{-1}I$. □

Proposição 3.17. *São válidas as seguintes propriedades:*

i) Se I é um ideal de A, então $I^{ec} = \bigcup_{s\in S} (I : s)$. Assim, $I^e = A$ se, e somente se, I intercepta S.

ii) A operação S^{-1} comuta com a formação de radicais.

Demonstração. i) $x \in I^{ec} = (S^{-1}I)^c$ se, e somente se, $x/1 = a/s$ para algum $a \in I, s \in S$ se, e somente se, $(xs - a)t = 0$, para algum $t \in S$ se, e somente se, $xst \in I$ se, e somente se, $x \in \bigcup_{s\in S} (I : s)$.

ii) Seja I um ideal de um anel A. Vamos provar que $S^{-1}Rad(I) = Rad(S^{-1}I)$. Seja $x/s \in S^{-1}(Rad(I))$, então $x \in Rad(I)$ e $s \in S$, logo $x^n \in I$ e $s^n \in S$, para algum inteiro positivo n. Assim, temos que $x^n/s^n = (x/s)^n \in S^{-1}I$, e então $x/s \in Rad(S^{-1}I)$. Portanto, $S^{-1}Rad(I) \subseteq Rad(S^{-1}I)$. Por outro lado, seja $y/t \in Rad(S^{-1}I)$, então $(y/t)^n = y^n/t^n \in S^{-1}I$, para algum $n > 0$, logo $y^n \in I$ e $t^n \in S$. Como $y^n \in I$, então $y \in Rad(I)$. Como $y/t \in Rad(S^{-1}I) \subseteq S^{-1}A$, então $y/t \in S^{-1}A$, logo $t \in S$. Assim, temos que $y/t \in S^{-1}Rad(I)$. Portanto, $Rad(S^{-1}I) \subseteq S^{-1}Rad(I)$. Como valem as duas inclusões, então temos que $Rad(S^{-1}I) = S^{-1}Rad(I)$.

□

Capítulo 4

Decomposição Primária

Neste capítulo, usaremos o conhecimento adquirido até aqui para estudar sobre a decomposição primária de ideais, que pode ser interpretada como a generalização da fatoração de um inteiro como produto de potências de números primos, assim como podemos visualizar um ideal primo de um anel A como a generalização de um número primo.

Definição 4.1. *Um ideal Q em um anel A é primário se $Q \neq A$ e se dado $xy \in Q$, então ou $x \in Q$ ou $y^n \in Q$, para algum $n > 0$.*

Proposição 4.2. *Todo ideal primo é um ideal primário.*

Demonstração. Seja P um ideal primo de um anel A. Dado $xy \in P$, temos que $x \in P$ ou $y \in P$, logo tomando $n = 1$ na definição de ideal primário, temos que $x \in P$ ou $y^n \in P$, portanto P é ideal primário. □

Exemplo 4.3. *Nem todo ideal primário é um ideal primo. De fato, seja $A = \mathbb{Z}$ e $Q = 4\mathbb{Z}$. Dado $xy \in Q$, temos que $xy = 4z = 2^2z$, para algum $z \in \mathbb{Z}$, logo por fatoração única temos que $x = 2^2w$ ou $y = 2^2w$ ou $x = 2w_1$ e $y = 2w_2$, para alguns $w, w_1, w_2 \in \mathbb{Z}$. Assim, temos que ou $x \in Q$ ou $y \in Q$ ou $x^2 \in Q$ e $y^2 \in Q$. Portanto, Q é um ideal primário de A. Mas Q não é um ideal primo de A, pois $20 = 2 \cdot 10 \in Q$, mas $2 \notin Q$ e $10 \notin Q$.*

Proposição 4.4. *Q é um ideal primário se, e somente se, $A/Q \neq 0$ e todo divizor de zero de A/Q for nilpotente.*

Demonstração. ($\Rightarrow$) Seja Q um ideal primário, então por definiçaõ $Q \neq A$, logo $A/Q \neq 0$. Seja $\overline{x}$ um divisor de zero de A/Q, então existe $\overline{y} \neq \overline{0}$ em A/Q tal que $\overline{y} \cdot \overline{x} = \overline{yx} = \overline{0}$, ou seja, $yx \in Q$, logo $y \in Q$ ou $x^n \in Q$. Como $\overline{y} \neq \overline{0}$, então $y \notin Q$, logo $x^n \in Q$, para algum $n > 0$, ou seja, $\overline{x}^n = \overline{0}$, logo $\overline{x}$ é nilpotente.

($\Leftarrow$) Suponha que $A/Q \neq 0$ e que todo divizor de zero de A/Q seja nilpotente. Como $A/Q \neq 0$, então $Q \neq A$. Seja $\overline{x} \in A/Q$ um divisor de zero, então existe $\overline{y} \neq \overline{0}$ em A/Q tal que $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{0}$, assim temos que $xy \in Q$ e como $\overline{x}$ é divisor de zero temos também que $\overline{x}$ é nilpotente em A/Q, ou seja, existe $m > 0$ tal que $\overline{x}^m = \overline{0}$, ou seja $x^m \in Q$. Logo, se $xy \in Q$ e $y \notin Q$, então $x^m \in Q$, portanto Q é primário. □

Proposição 4.5. *A contração de um ideal primário é um ideal primário.*

Demonstração. Seja $f : A \to B$ um homomorfismo de anéis e Q um ideal primário de B, queremos mostrar que $f^{-1}(Q)$ é um ideal primário de A. A prova de que $f^{-1}(Q)$ é ideal de A já foi feita na Proposição 1.42, resta provar que este ideal é primário. Sejam $x, y \in A$ tais que $x \cdot y \in f^{-1}(Q)$. Então, $f(x \cdot y) = f(x) \cdot f(y) \in Q$ e como Q é ideal primário de B, então $f(x) \in Q$ ou $(f(y))^n = f(y^n) \in Q$, para algum $n > 0$, ou seja, $x \in f^{-1}(Q)$ ou $y^n \in f^{-1}(Q)$. Portanto, $f^{-1}(Q)$ é ideal primário de A. □

Proposição 4.6. *Seja $f : A \to B$ um homomorfismo de anéis e Q um ideal primário de B, então $A/f^{-1}(Q)$ é isomorfo a um subanel de B/Q.*

Demonstração. Considere a função $\phi : A/f^{-1}(Q) \to B/Q$ definida por $\phi(x + f^{-1}(Q)) = f(x) + Q$, onde $x \in A$. Como f é um homomorfismo de anéis, temos que ϕ também é, e pelo exemplo 1.7 temos que $Im(\phi) = \{f(a) + Q : f(a) \in f(A)\}$ é um subanel de B/Q. Note que $ker(\phi) = \{x + f^{-1}(Q) : f(x) + Q = \overline{0}\} = \{x + f^{-1}(Q) : f(x) \in Q\} = \{x + f^{-1}(Q) : x \in f^{-1}(Q)\} = 0 + f^{-1}(Q)$. Assim, pelo Teorema 1.16, temos que $A/ker(\phi) \simeq Im(\phi)$, e portanto $A/f^{-1}(Q) \simeq \{f(a) + Q : f(a) \in f(A)\}$. □

Proposição 4.7. *Seja Q um ideal primário de um anel A. Então o radical de Q, que denotamos por $Rad(Q)$, é o menor ideal primo contendo Q.*

Demonstração. Pela Proposição 1.81 sabemos que o radical de Q é a interseção dos ideais primos de A que contêm Q, portanto basta mostrar que o $Rad(Q)$ é de fato um ideal primo. Seja $xy \in Rad(Q)$, então $(xy)^m = x^m y^m \in Q$, para algum $m > 0$, e portanto ou $x^m \in Q$ ou $y^{mn} \in Q$, para algum $n > 0$, isto é, ou $x \in Rad(Q)$ ou $y \in Rad(Q)$. Portanto $Rad(Q)$ é um ideal primo de A, como queríamos provar. □

Exemplo 4.8. *Os ideais primários de $\mathbb{Z}$ são (0) e (p^n), onde p é um número primo. De fato, pelo Exemplo 1.41, sabemos que o ideal (0) é um ideal primo de $\mathbb{Z}$, e então, pela Proposição 4.2, (0) é um ideal primário de $\mathbb{Z}$. O ideal (p^n) também é um ideal primário de $\mathbb{Z}$, pois dado $xy \in (p^n)$, temos que $xy = p^n m$, para algum $m > 0$, logo $p \mid x$ ou $p \mid y$, e portanto ou $x^i \in (p^n)$ ou $y^i \in (p^n)$, para algum $i > 0$, e portanto, (p^n) é um ideal primário de $\mathbb{Z}$. Estes são os únicos ideais primários de $\mathbb{Z}$, pois são os únicos ideais de $\mathbb{Z}$ cujo radical é primo. De fato, como todo ideal de $\mathbb{Z}$ é gerado por um*

único elemento, seja I um ideal de $\mathbb{Z}$ tal que $I = (z) = (\prod_{i=1}^{n} p_i^{r_i})$, então $Rad(I) = (\prod_{i=1}^{n} p_i)$. Logo, se $n \geq 2$, então $Rad(I)$ não é primo, pois $\prod_{i=1}^{n} p_i \in (\prod_{i=1}^{n} p_i)$, mas $p_i \notin (\prod_{i=1}^{n} p_i)$, para todo i.

Definição 4.9. *Se Q é primário e $Rad(Q) = P$, onde P é um ideal primo do anel A, dizemos que Q é P-primário.*

Proposição 4.10. *Seja I um ideal do anel A, se $Rad(I)$ é um ideal maximal, então I é um ideal primário. Em particular, as potências de um ideal maximal M são M-primárias.*

Demonstração. Seja $Rad(I) = M$, onde M é um ideal maximal de A. Se $\pi : A \to A/I$ é a projeção canônica, então segue da Proposição 1.79 que $M = Rad(I) = \pi^{-1}(\mathcal{N}(A/I))$. Como π é sobrejetor, então $\pi(M) = \pi(\pi^{-1}(\mathcal{N}(A/I))) = \mathcal{N}(A/I)$. Pelo item i) da Proposição 1.80, sabemos que $I \subseteq Rad(I) = M$, logo pelo Teorema 1.17, temos que $\frac{A/I}{M/I} \simeq A/M$. Como M é maximal, temos pelo item i) da Proposição 1.39 que A/M é corpo, logo $\frac{A/I}{M/I}$ é corpo e, novamente pelo item i) da Proposição 1.39, segue que $M/I = \pi(M) = \mathcal{N}(A/I)$ é maximal e portanto $\mathcal{N}(A/I)$ é maximal. Assim, dado um ideal primo P de A/I, segue pela Proposição 1.54 que $\mathcal{N}(A/I) \subseteq P$, o que implica que $\mathcal{N}(A/I) = P$, uma vez que $\mathcal{N}(A/I)$ é maximal. Desta forma, o anel A/I tem somente um ideal primo. Então, todo elemento de A/I ou está no ideal maximal $\mathcal{N}(A/I)$ e portanto é nilpotente ou não está em um ideal maximal de A/I e portanto, pelo Corolário 1.48, é uma unidade. Assim, segue que todo divisor de zero de A/I é nilpotente, pois caso contrário ele seria uma unidade, ou seja, dado um divisor de zero $\overline{x} \in A/I$, se $\overline{x}$ é uma unidade, então existe $\overline{x}^{-1} \in A/I$, tal que $\overline{x} \cdot \overline{x}^{-1} = \overline{1}$, e como $\overline{x}$ é divisor de zero, então existe $\overline{y} \in A/I$, com $\overline{y} \neq \overline{0}$, tal que $\overline{y} \cdot \overline{x} = \overline{0}$, logo $\overline{x} \cdot \overline{x}^{-1} = \overline{1}$, o que implica $\overline{y} \cdot \overline{x} \cdot \overline{x}^{-1} = \overline{y} \cdot \overline{1}$, portanto $\overline{0} = \overline{y}$. Absurdo! Logo todo divisor de zero de A/I é de fato nilpotente. Pela Proposição 4.4 isto implica que I é ideal primário, como queríamos provar. Por outro lado, se M é ideal maximal e, portanto, ideal primo, temos pelo item vii) da Proposição 1.80 que $M = Rad(M^n)$, para todo $n > 0$, logo M^n é M-primário para todo $n > 0$. □

Lema 4.11. *Se Q_i, com $1 \leq i \leq n$, são ideais P-primários, então $Q = \bigcap_{i=1}^{n} Q_i$ é P-primário.*

Demonstração. Para mostrar que Q é P-primário devemos mostrar que $Rad(Q) = P$ e que Q é primário. Pelo item iii) da Proposição 1.80, temos que $Rad(Q) = Rad(\bigcap_{i=1}^{n} Q_i) = \bigcap Rad(Q_i) = P$. Agora, seja $xy \in Q$, com $y \notin Q$. Então para algum i, temos que $xy \in Q_i$ e $y \notin Q_i$, portanto $x^n \in Q_i$, e então $x \in P$, uma vez que Q_i é P-primário. Portanto Q é primário. □

Lema 4.12. *Seja Q um ideal P-primário e x um elemento do anel A. Então:*

i) se $x \in Q$, então $(Q : x) = A$.

ii) se $x \notin Q$, então $(Q : x)$ é P-primário, e portanto $Rad(Q : x) = P$.

iii) se $x \notin P$, então $(Q : x) = Q$.

Demonstração. *i)* Seja $x \in Q$, então $(Q : x) = \{a \in A : ax \in Q\} = A$, pois Q é ideal de A.

ii) Suponha que $y \in (Q : x)$, então $xy \in Q$. Como, por hipótese, $x \notin Q$, então existe um inteiro positivo n, tal que $y^n \in Q$. Como P contém Q, então $y^n \in P$, e como P é primo, temos que $y \in P$. Logo, $Q \subseteq (Q : x) \subseteq P$. Tomando radicais, temos que $Rad(Q) \subseteq Rad(Q : x)$ e como $Rad(Q) = P$, segue que $P \subseteq Rad(Q : x) \subseteq P$, logo $Rad(Q : x) = P$. Agora, seja $yz \in (Q : x)$ e suponha que nenhuma potência de y pertença a $(Q : x)$. Desta forma, precisamos provar que $z \in (Q : x)$. Por definição, se $yz \in (Q : x)$, então $xyz \in Q$. Como Q é primário e nenhum potência positiva de y pentence a Q, então $xz \in Q$, o que implica em $z \in (Q : x)$, como queríamos provar. Portanto, $(Q : x)$ é P-primário.

iii) Se $x \notin P$, então $(Q : x) = \{a \in A : ax \in Q\} = Q$, pois Q é P-primário e não existe $n > 0$ tal que $x^n \in Q$.

□

4.1 Decomposição Primária de Ideais

Definição 4.13. *Uma decomposição primária de um ideal I de A é uma expressão de I como uma interseção finita de ideais primários, isto é, $I = \bigcap_{i=1}^{n} Q_i$, onde Q_i são ideais primários.*

Definição 4.14. *Um ideal I é dito decomponível se admite uma decomposição primária.*

Exemplo 4.15. *Vamos verificar que o ideal $I = (96)$ do anel $\mathbb{Z}$ é decomponível. Seja, $a \in I$, então $a = 96x$, para algum $x \in \mathbb{Z}$. Note que, $a = 96x = 2^5 \cdot (3x) = 3 \cdot (2^5 x)$, ou seja, $a \in (2^5) \cap (3)$. Por outro lado, se $a \in (2^5) \cap (3)$, temos que $a = 2^5 x$ e $a = 3y$, com $x, y \in \mathbb{Z}$. Contudo, o mínimo múltiplo comum de 2^5 e 3 é 96, ou seja, a é um múltiplo de 96, isto é, $a \in (96)$. Portanto, $I = (96)$ é um ideal que admite uma decomposição primária, e tal decomposição é $I = (2^5) \cap (3)$.*

Definição 4.16. *A decomposição primária de um ideal decomponível $I = \bigcap_{i=1}^{n} Q_i$ é dita ser minimal se, para todo $i \in \{1, \ldots, n\}$, tivermos que:*

i) Todos os $Rad(Q_i)$ forem distintos;

ii) Tivermos que $\bigcap_{j \neq i} Q_j \not\subseteq Q_i$, para $1 \leq i \leq n$.

Proposição 4.17. *Toda decomposição primária pode ser reduzida a uma decomposição primária minimal.*

Demonstração. Dada uma decomposição primária $I = \bigcap_{i=1}^{n} Q_i$, onde $Rad(Q_k) = Rad(Q_l) = P$, com $k \neq l$, temos pelo Lema 4.11, que podemos obter um novo ideal P-primário $Q_m = Q_k \cap Q_l$. Repetindo este processo sempre que houver dois ideais com mesmo radical na decomposição primária de I, iremos obter uma decomposição primária satisfazendo a condição i) da definição de decomposição primária minimal, sem mudar a decomposição de I. Feito isso, podemos omitir qualquer termo desnecessário para obter a condição ii) da seguinte forma: suponhamos que $\bigcap_{j\neq i} Q_j \subseteq Q_i$, então $\bigcap_{j\neq i} Q_j = \bigcap_j Q_j = I$. Então, segue que podemos tirar Q_i. Portanto, toda decomposição primária pode ser reduzida a uma decomposição primária minimal. □

Teorema 4.18 (1^{o} Teorema da Unicidade)**.** *Seja I um ideal decomponível e seja $I = \bigcap_{i=1}^{n} Q_i$ uma decomposição primária minimal de I. Seja $P_i = Rad(Q_i)$, para $1 \leq i \leq n$. Então os P_i's são precisamente os ideais primos do conjunto de ideais $\{Rad(I : x); x \in A\}$, e portanto não dependem da decomposição particular de I.*

Demonstração. Pelo item iv) da Proposição 1.77, para cada $x \in A$, temos que $(I : x) = (\bigcap_{i=1}^{n} Q_i : x) = \bigcap_{i=1}^{n}(Q_i : x)$. Portanto, pelo item iii) da Proposição 1.80, temos que $Rad(I : x) = Rad(\bigcap_{i=1}^{n}(Q_i : x)) = \bigcap_{i=1}^{n} Rad(Q_i : x)$ e, pelo item ii) do Lema 4.12, temos que $\bigcap_{i=1}^{n} Rad(Q_i : x) = \bigcap_{x\notin Q_j} P_j$, portanto $Rad(I : x) = \bigcap_{x\notin Q_j} P_j$. Suponha que $Rad(I : x)$ seja primo; então, segue da Proposição 1.73 que $Rad(I : x) = P_j$, para algum j. Logo, todo ideal primo da forma $Rad(I : x)$ é um dos P_j. Reciprocamente, para cada i existe $x_i \notin Q_i$, com $x_i \in \bigcap_{j\neq i} Q_j$, uma vez que a decomposição é minimal. Portanto, temos que $Rad(I : x_i) = \bigcap_{x_i\notin Q_j} P_j = P_i$. □

Observação 4.19. *Pela parte final da demonstração do Teorema acima, temos que para cada i, com $1 \leq i \leq n$, existe um $x_i \in A$ tal que $x_i \notin Q_i$ e $x_i \in \bigcap_{j\neq i} Q_j$. Temos também que $(I : x_i) = \bigcap_{j=1}^{n}(Q_j : x_i)$. Pelo item i) do Lema 4.12, temos que $(Q_j : x_i) = A$, para $i \neq j$. Logo, $(I : x_i) = (Q_i : x_i)$, e pelo item ii) do Lema 4.12, temos que $(I : x_i)$ é P_i-primário.*

Definição 4.20. *Os ideiais primos P_i dados no Teorema 4.18 são chamados ideias associados ou pertencentes a I. Os elementos minimais do conjunto $\{P_1, ..., P_n\}$ são chamados ideais primos isolados pertencentes a I. Os ideais primos do conjunto $\{P_1, ..., P_n\}$ que não são isolados são chamados ideais primos mergulhados.*

Observação 4.21. *Um ideal decomponível I é primário se, e somente se, ele tem apenas um ideal primo associado.*

Proposição 4.22. *Seja I um ideal decomponível. Então, todo ideal primo $P \supseteq I$ contém um ideal primo isolado associado a I. Logo, os ideais primos isolados de I são precisamente os elementos minimais do conjunto de todos os ideias primos contendo I.*

Demonstração. Se $P \supseteq I = \bigcap_{i=1}^{n} Q_i$, então temos, pelos item *vii)* e *iii)* da Proposição 1.80, que $P = Rad(P) \supseteq Rad(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} Rad(Q_i) = \bigcap_{i=1}^{n} P_i$. Logo, pelo item *ii)* da Proposição 1.73, temos que $P \supseteq P_i$ para algum i e, portanto, P contém um ideal primo associado a I. Se P_i for isolado o resultado está provado, caso contrário, então P_i não é um elemento minimal do conjunto $\{P_1, ..., P_n\}$, logo existe $P_j \in \{P_1, ..., P_n\}$ tal que $P_j \subsetneq P_i \subseteq P$. Se P_j for isolado o resultado está provado, caso contrário, continuamos o processo até encontrar um ideal isolado, o que ocorrerá em algum momento, uma vez que o conjunto $\{P_1, ..., P_n\}$ é finito. □

Proposição 4.23. *Sejam I um ideal decomponível, $I = \bigcap_{i=1}^{n} Q_i$ uma decomposição primária minimal e $Rad(Q_i) = P_i$. Então, $\bigcup_{i=1}^{n} P_i = \{x \in A; (I : x) \neq I\}$. Em particular, se o ideal nulo (0) é decomponível, então o conjunto D dos divisores do zero de A é a união de todos os ideais primos pertencentes a (0).*

Demonstração. Se I é decomponível, então (0) é decomponível em A/I. De fato, escrevemos $(0) = \bigcap \overline{Q_i}$, onde $\overline{Q_i}$ é a imagem de Q_i em A/I pela projeção canônica $\pi : A \to A/I$. Provemos que a projeção canônica é primária. Seja J um ideal primário de A que contém I. Se $\overline{ab} \in J/I = \overline{J}$, então $ab \in J$, e como J é primário então $a \in J$ ou $b^n \in J$. Logo, $\overline{a} \in \overline{J}$ ou $\overline{b}^n \in \overline{J}$, assim $\overline{J}$ é primário. Portanto, para demonstrar esta proposição, é suficiente mostrar apenas que se (0) é decomponível, então o conjunto D dos divisores do zero de A é a união de todos os ideais primos pertencentes a (0). Pela Proposição 1.83, temos que $D = \bigcup_{x \neq 0} Rad(Ann(x)) = \bigcup_{x \neq 0} Rad(0 : x)$. Da demonstração do Teorema 4.18, temos que $Rad(0 : x) = \bigcap_{x \notin Q_j} P_j \subseteq P_j$, para algum j, portanto $D \subseteq \bigcup_{i=1}^{n} P_i$. Mas novamente pelo Teorema 4.18, temos que cada P_i é da forma $Rad(0 : x)$, para algum $x \in A$, portanto $\bigcup P_i \subseteq D$. □

Agora, vamos investigar o comportamento dos ideias primários sob localização.

Proposição 4.24. *Seja S um conjunto multiplicativamente fechado de A, e seja Q um ideal P-primário. Temos que:*

i) Se $S \cap P \neq \emptyset$, então $S^{-1}Q = S^{-1}A$.

ii) Se $S \cap P = \emptyset$, então $S^{-1}Q$ é $S^{-1}P$-primário e sua contração em A é Q.

Demonstração. i) Se $s \in S \cap P$, então $s^n \in S \cap Q$, para algum $n > 0$. Portanto, $S^{-1}Q$ contém $\frac{s^n}{1}$, que é uma unidade em $S^{-1}A$.

ii) Se $S \cap P = \emptyset$, pelo item *iii)* do Lema 4.12, temos que $(Q : s) = Q$, para todo $s \in S$. Portanto, pelo item *i)* da Proposição 3.17, temos que $Q^{ec} = \bigcup_{s \in S} (Q : s) = Q$. Pelo item *ii)* da Proposição 3.17,

temos que $Rad(S^{-1}Q) = S^{-1}Rad(Q) = S^{-1}P$. Agora, vamos verificar que $S^{-1}Q$ é primário. Seja $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}Q$, então existem $q \in Q$ e $u \in S$ tais que $\frac{ab}{st} = \frac{q}{u}$. Assim, existe $v \in S$ tal que $v(abu - stq) = 0$, logo $vuab = vstq \in Q$. Como Q é primário, então $ab \in Q$ ou $vu \in P$, mas $S \cap P = \emptyset$, logo $ab \in Q$. Isso implica que $a \in Q$ ou $b \in P$. Assim, $\frac{a}{s} \in S^{-1}Q$ ou $\frac{b}{t} \in S^{-1}P = Rad(S^{-1}Q)$. Portanto $S^{-1}Q$ é primário, e como $Rad(S^{-1}Q) = S^{-1}P$, segue que $S^{-1}Q$ é $S^{-1}P$-primário.

□

Notação: *Para qualquer ideal I e qualquer subconjunto multiplicativamente fechado S em A, vamos denotar a contração em A do conjunto $S^{-1}I$ por $S(I)$.*

Definição 4.25. *Um conjunto Σ de ideais primos associados a I é dito isolado se satisfaz a seguinte condição: se P' é um ideal primo associado a I e $P' \subseteq P$, para algum $P \in \Sigma$, então $P' \in \Sigma$.*

Observação 4.26. *Seja Σ um conjunto isolado de ideais primos associados a I e $S = A - \bigcup_{P\in\Sigma} P$. Então S é um conjunto multiplicativamente fechado e, para qualquer ideal primo P' associado a I, temos que se $P' \in \Sigma$, então $P' \cap S = \emptyset$. Agora, se $P' \notin \Sigma$, então $P' \not\subseteq \bigcup_{P\in\Sigma} P$, pois caso contrário, teríamos pelo item i) da Proposição 1.73 que $P' \subseteq P$, para algum $P \in \Sigma$, o que implicaria que $P' \in \Sigma$, o que seria uma contradição. Assim, temos que $P' \cap S \neq \emptyset$.*

Teorema 4.27 (2º Teorema da Unicidade)**.** *Sejam I um ideal decomponível de um anel A, $I = \bigcap_{i=1}^{n} Q_i$ uma decomposição primária minimal de I e $\Sigma = \{P_{i_1}, ..., P_{i_m}\}$ um conjunto isolado de ideais primos associados a I. Então, $Q_{i_1} \cap ... \cap Q_{i_m}$ é independente da decomposição.*

Demonstração. Seja $S = A - P_{i_1} \cup \cdots \cup P_{i_m}$. Temos que $S^{-1}I = S^{-1}(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} S^{-1}Q_i$ (pelo item *ii*) do Corolário 3.15). Para todo i tal que $Rad(Q_i) \notin \Sigma$, temos $S \cap Rad(Q_i) \neq \emptyset$ e, pelo item *i*) da Proposição 4.24, temos que $S^{-1}Q_i = S^{-1}A$. Logo, $S^{-1}I = \bigcap_{j=1}^{m} S^{-1}Q_{i_j}$. Como $S \cap P_{i_j} = \emptyset$, então pelo item *ii*) da Proposição 4.24, segue que $S(Q_{i_j}) = Q_{i_j}$. Assim, temos que $S(I) = (S^{-1}I)^c = (\bigcap_{j=1}^{m} S^{-1}(Q_{i_j}))^c = \bigcap_{j=1}^{m}(S^{-1}(Q_{i_j}))^c$ (pela Proposição 1.87). Daí, $S(I) = \bigcap_{j=1}^{m} S(Q_{i_j}) = \bigcap_{j=1}^{m} Q_{i_j}$. Portanto $\bigcap_{j=1}^{m} Q_{i_j}$ depende apenas de I e do conjunto Σ, já que S depende apenas de Σ. □

Corolário 4.28. *As componentes primárias isoladas, isto é, as componentes primárias Q_i correspondentes aos ideais primos isolados P_i, são unicamente determinadas por I.*

4.2 Decomposição Primária em Anéis Noetherianos

Vimos até agora, resultados que garantem a unicidade da decomposição primária de ideais decomponíveis. Nesta seção, veremos que em um anel Noetheriano temos também a garantia da existência

desta decomposição.

Definição 4.29. *Um anel A é dito Noetheriano se satisfaz uma das seguintes condições:*

i) Todo conjunto não vazio de ideais em A tem um elemento maximal.

ii) Toda cadeia ascendente de ideais de A é estacionária.

iii) Todo ideal de A é finitamente gerado.

Proposição 4.30. *As três condições da definição anterior são equivalentes.*

Demonstração. *i)* $\Rightarrow$ *ii)* Aplicando a condição maximal ao conjunto de ideais de uma cadeia ascendente $\{I_j; j \geq 1\}$, com $I_j \subseteq I_{j+1}$, temos que se I_n é o elemento maximal deste conjunto, então a cadeia ascendente de ideais é estacionária em I_n, isto é, $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n = I_{n+1} = I_{n+2} = \cdots$.

ii) $\Rightarrow$ *iii)* Vamos provar pela contra-recíproca. Seja I um ideal de A que não é finitamente gerado. Então existem $a_1, \ldots, a_r, \ldots \in I$, tais que $\langle a_1, \ldots, a_j \rangle \neq I$, para todo inteiro positivo j, e ainda $a_{j+1} \notin \langle a_1, \ldots, a_j \rangle$. Logo, conseguimos construir uma cadeia $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \cdots$ ascendente e não estacionária.

iii) $\Rightarrow$ *ii)* Seja $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ uma cadeia ascendente de ideais de A. Sabemos que $I := \bigcup_{j=1}^{\infty} I_j$ também é um ideal de A. Por hipótese, existem $a_1, a_2, \ldots, a_r \in A$ tais que $I = \langle a_1, \ldots, a_r \rangle$. Logo, para n suficientemente grande temos que $a_i \in I_n$ para todo $i \in \{1, \ldots, r\}$ e, consequentemente, $I = I_n = I_{n+1} = \cdots$.

ii) $\Rightarrow$ *i)* Suponha que existe um conjunto não vazio Σ de ideais de A sem elemento maximal. Logo, para cada ideal $I_1 \in \Sigma$, existe um ideal $I_2 \in \Sigma$ tal que $I_1 \subsetneq I_2$. Desta maneira conseguimos construir uma cadeia ascendente de ideais não estacionária.

□

Exemplo 4.31. *Todo domínio de ideais principais (e portanto também os corpos) satisfazem a condição iii) da Definição 4.29 e portanto são anéis Noetherianos.*

Definição 4.32. *Sejam I, J e K ideais de um anel A. O ideal I é dito ser irredutível se toda vez que $I = J \cap K$, então ou $I = J$ ou $I = K$.*

Lema 4.33. *Em um anel Noetheriano A, todo ideal é uma interseção finita de ideais irredutíveis.*

Demonstração. Seja U o conjunto dos ideais do anel A que não são interseções finitas de ideais irredutíveis. Suponha que $U \neq \emptyset$. Então, pelo item i) da definição de anel Noetheriano, sabemos que U possui um elemento maximal I. Como I é redutível, segue que $I = J \cap K$, no qual $I \subsetneq J$ e $I \subsetneq K$. Pela maximalidade de I temos que $J \notin U$ e $K \notin U$, ou seja, J e K são interseções finitas de ideais irredutíveis, assim I é interseção finita de ideais irredutíveis. Contradição! Portanto, $U = \emptyset$. □

Lema 4.34. *Em um anel Noetheriano A, todo ideal irredutível é um ideal primário.*

Demonstração. Passando ao anel quociente, que também é Noetheriano conforme provado na página 415 da referência [5], é suficiente verificar que se o ideal nulo é irredutível, então ele é primário. Seja $xy \in (0)$, com $y \neq 0$, vamos mostrar que $x^m \in (0)$ para algum $m \in \mathbb{Z}$, com $m > 0$. Considere a cadeia de ideais $Ann(x) \subseteq Ann(x^2) \subseteq \cdots$. Pela condição da cadeia ascendente, esta cadeia é estacionária, ou seja, existe $n \in \mathbb{Z}$, com $n > 0$, tal que $Ann(x^n) = Ann(x^{n+1}) = \cdots$. Segue então que $(x^n) \cap (y) = (0)$, pois se $a \in (y)$, então existe $c \in A$ tal que $a = cy$, logo $ax = cyx = 0$ e se $a \in (x^n)$, então existe $b \in A$ tal que $a = bx^n$, logo $ax = bx^{n+1} = 0$, o que implica que $b \in Ann(x^{n+1}) = Ann(x^n)$. Assim $bx^n = 0$, ou seja, $a = 0$. Como (0) é irredutível, de $(0) = (x^n) \cap (y)$ e $(y) \neq (0)$, devemos ter $x^n = 0$, e portanto temos que (0) é primário. □

Teorema 4.35. *Em um anel Noetheriano A, todo ideal admite uma decomposição primária.*

Demonstração. Pelo Lema 4.33, em um anel Noetheriano A, todo ideal é uma interseção finita de ideais irredutíveis, e portanto, pelo Lema 4.34, todo ideal é uma interseção finita de ideais primários, logo todo ideal admite uma decomposição primária. □

Observação 4.36. *Com este último Teorema, concluímos que todos os resultados estudados na seção 4.1 são válidos para Anéis Noetherianos.*

Considerações finais

Com o estudo detalhado de anéis, ideais e módulos, pôde-se ter uma boa base do que é a Álgebra Comutativa. Estes conjuntos tão importantes na área de Álgebra, abrem portas para o desenvolvimento de várias outras teorias. A forma como os conceitos, propriedades e resultados se conectaram e possibilitaram o estudo da decomposição primária de ideais, mostra como a Matemática é diversa e como resultados complexos podem ser entendidos sem grandes dificuldades, desde que sejam analisados minuciosamente e que os conceitos sejam construídos de forma clara e precisa.

Referências Bibliográficas

[1] Atiyah, M. F. and Macdonald, I. G. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Massachusetts, 1969.

[2] Gonçalves, F. S. *Introdução à Geometria Algébrica*. Trabalho de Conclusão de Curso (Graduação em Matemática) - Departamento de Matemática, Universidade Federal de São Carlos. São Carlos, 2010.

[3] Souza, L. D. *Sequências exatas e aplicações: o Lema da Cobra*. Trabalho de Conclusão de Curso (Graduação em Matemática) - Departamento de Matemática, Universidade Federal de Santa Catarina. Florianópolis, 2017.

[4] Halmos, P. R. *Naive Set Theory*. Van Nostrand, Princeton, 1960.

[5] Lang, S. *Algebra*. 3rd ed., Springer-Verlag, New York, 2002.