UNIVERSIDADE FEDERAL DE OURO PRETO

DEPARTAMENTO DE MATEMÁTICA

Mônica Madeira dos Santos

Decomposição Primária em Aneis Noetherianos

Ouro Preto, Brasil

2022

UNIVERSIDADE FEDERAL DE OURO PRETO

Mônica Madeira dos Santos

Decomposição Primária em Aneis Noetherianos

Monografia submetida ao Curso de Matemática da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do Grau de Graduado em Bacharelado em Matemática.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira

Universidade Federal de Ouro Preto – UFOP

Instituto de Ciências Exatas e Biológicas

Departamento de Matemática

Ouro Preto, Brasil

2022

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
COLEGIADO DO CURSO DE BACHARELADO EM MATEMATICA

FOLHA DE APROVAÇÃO

Mônica Madeira dos Santos

Decomposição primária em Anéis Noetherianos

Monografia apresentada ao Curso de Bacharelado em Matemática da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharela em Matemática

Aprovada em 27 de outubro de 2022

Membros da banca

Dr. Edney Augusto Jesus de Oliveira - Orientador- Universidade Federal de Ouro Preto
Dr.ª Ana Paula da Silva Cota - Universidade Federal de Ouro Preto
Dr. Savio Ribas - Universidade Federal de Ouro Preto

Edney Augusto Jesus de Oliveira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 24/11/2022.

Documento assinado eletronicamente por **Edney Augusto Jesus de Oliveira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 24/11/2022, às 16:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0420186** e o código CRC **DF14DEF8**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1312 - www.ufop.br

Agradecimentos

Primeiro agradeço a Deus pelo dom da vida e pela oportunidade de todos os dias acordar e ter a chance de ser melhor do que ontem. Agradeço a minha mãe Mirna (in memoriam) e o meu pai Orlando por terem sido o alicerce necessário para a realização desse sonho.
Gostaria de agradecer também ao melhor grupo de amigos desse curso, #vaitime, que ao longo dos anos foi só crescendo e se tornando essencial durante essa graduação, em especial, agradeço as minhas melhores amigas Bárbara e Stefani que choraram, torceram, lutaram e estiveram comigo nos meus melhores e piores momentos e me acompanham desde o início dessa caminhada dentro e fora da UFOP. Vocês são vitais pra mim. Agradeço ao Pedro, o meu melhor amigo ao longo desse curso que me proporcionou n-ésimos puxões de orelha por acreditar no meu potencial, por ter o melhor abraço do mundo, e ter a alma mais linda que eu já senti. A Ana Tw pela pessoa incrível que é e que por todas as nossas conversas e desabafos, reconheço nela uma irmã de alma. A gente cuida dos nossos. Aos demais colegas e amigos de curso que me acompanharam e tornaram a jornada até aqui mais leve e feliz, minha eterna gratidão.

Agradeço ao meu orientador Edney por toda paciência, empatia, amizade, conselhos e dedicação ao longo da minha trajetória como aluna do bacharelado e principalmente durante o desenvolvimento desse trabalho. Obrigada por ter acreditado em mim em momentos que eu mesma não fui capaz de acreditar.

Aos meus amigos Caio e Carolina por sempre acreditarem em mim e me apoiarem ao longo dessa jornada. Vocês são os melhores! Ao PETMAT e o Centro Acadêmico (Gestão Gauss e Mobiüs) por terem me proporcionado a experiência e o amadurecimento necessário para que eu pudesse chegar até aqui.

A minha amada república TchuTchuTchu por ser um lugar de acolhimento e aprendizado ao longo desses anos e no qual tenho orgulho de chamar de lar. Amo vocês tchucas.

A todos os professores que ao longo dessa graduação proporcionaram ensinamentos que vão além da sala de aula, meu respeito, carinho e gratidão. Por fim, aos membros da banca, obrigado por aceitarem o convite e dedicarem um tempo a este trabalho.

À minha mãe Mirna (in memoriam) e minha tia Myriam (in memoriam) pelo amor e apoio incondicional.

"Por que caímos, Bruce? Para aprendermos a levantar."

Thomas Wayne - Batman Begins

Resumo

Nesta monografia estudaremos a decomposição primária de ideais em aneis Noetherianos. Faremos aqui um breve estudo de aneis e ideais, apresentaremos o conceito de anel Noetheriano e sua caracterização, e em seguida mostraremos uma prova do *Teorema da Base de Hilbert*. Além disso, vamos definir uma decomposição primária deduzindo seus respectivos resultados através dos ideais primários e radicais. Por fim, exibiremos resultados que garantirão a existência de uma decomposição primária em aneis Noetherianos.

Palavras-chave: Aneis Noetherianos. Ideais Primários. Decomposição Primária.

Abstract

In this monograph we will study the primary decomposition of ideals in Noetherian rings. We will make here a brief study of rings and ideals, we will present the Noetherian ring concept and its characterization, and then we will show a proof of *Hilbert's Basis Theorem*. Furthermore, we will define a primary decomposition by deducing its respective results through the primary and radical ideals. Finally, we will show results that will ensure the existence of a primary decomposition in Noetherian rings.

Keywords: Noetherian Rings. Primary Ideals. Primary Decomposition.

Sumário

Introdução

A Álgebra Comutativa é essencialmente o estudo dos aneis comutativos, desenvolvendo-se respectivamente a partir da Geometria Algébrica e da Teoria Algébrica dos Números. Na primeira vertente, o modelo dos aneis estudados é o anel de polinômios em diversas variáveis sobre um corpo $\mathbb{K}$ enquanto que na segunda, o modelo é o anel dos inteiros racionais (ATIYAH M.F; MACDONALF, 1969, Adaptado).

Em uma grande classe de aneis comutativos, incluindo todos os aneis Noetherianos, todo ideal possui uma decomposição primária, que é uma decomposição semelhante, mas permite ideais que são análogos às potências de primos. Esta decomposição pode ser considerada como uma generalização da fatoração de um inteiro n em $\mathbb{Z}$ como produto de potências de primos através dos ideais primários (DUMMIT; FOOTE, 2003, página 681).

A presente monografia tem como objetivo o estudo da decomposição primária de ideais em aneis Noetherianos e, para isto, apresentamos primeiramente no Capítulo 1 tópicos da Teoria de Conjuntos e Teoria de Aneis cujos resultados relativos a Teoria de Ideais serão amplamente explorados ao longo do nosso trabalho. Nesse capítulo, dois ideais que recebem destaque na Álgebra Comutativa: o *Nilradical* e o *Radical de Jacobson* de um anel A cujas caracterizações decorrem das definições relativas aos ideais maximais e primos.

O objetivo do Capítulo 2 é definir e caracterizar os aneis Noetherianos sob várias operações familiares da teoria de aneis, em particular, provamos o famoso *Teorema da Base de Hilbert* além de apresentarmos algumas deduções importantes da condição noetheriana.

No Capítulo 3, apresentamos os principais resultados que nos auxiliam para o desenvolvimento dos pontos apresentados sobre a decomposição primária de um ideal em um anel A, em particular, em aneis Noetherianos, tais como ideais radicais e ideais primários, a definição de decomposição primária, ideais P-primários além dos teoremas de unicidade de tal decomposição.

As principais referências para o desenvolvimento desta monografia foram (ATIYAH M.F; MACDONALF, 1969) e (MARTIN, 2014).

1 Base Teórica

Apresentamos neste capítulo os resultados mais pertinentes para o desenvolvimento do nosso trabalho relativos à teoria de conjuntos e à teoria de aneis. As principais referências deste capítulo foram (CONRAD, 2020), (DOMINGUES; IEZZI, 2003), (HALMOS, 1970), (LEQUAIN Y; GARCIA, 2005) e (HEFEZ, 2016).

1.1 Teoria de Conjuntos

Nesta seção, apresentamos conceitos da teoria de conjuntos referentes a relação de ordem, elemento maximal, condição de cadeia e o Lema de Zorn, uma vez que tais conceitos são utilizados em alguns resultados envolvendo a decomposição primária em anéis noetherianos.

Definição 1. *Seja I um conjunto não vazio qualquer. Uma* ***família indexada por I*** *é uma coleção de conjuntos A_i com $i \in I$.*

Notação: $\{A_i\}_{i\in I}$.

Definição 2. *Definimos o* ***par ordenado*** *de a e b, com a sendo a primeira coordenada e b sendo a segunda coordenada, o conjunto (a, b) definido por:*

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Proposição 1. *Se (a, b) e (x, y) são pares ordenados e se $(a, b) = (x, y)$, então $a = x$ e $b = y$.*

A demonstração dessa proposição pode ser consultada em (HALMOS, 1970, página 24).

Definição 3. *Sejam A, B dois conjuntos não vazios. Definimos o* ***produto cartesiano*** *de A e B, como o conjunto de todos os pares ordenados em que a primeira coordenada pertence a A e a segunda a B.*

$$\textit{Notação: } A \times B = \{x;\ x = (a, b) \mid a \in A \text{ e } b \in B\}.$$

Observação 1. *Todo conjunto de pares ordenados é um subconjunto de um produto cartesiano de dois conjuntos.*

Fazendo uso de pares ordenado, podemos aqui estabelecer a ideia de relação entre conjuntos, dita relação binária.

Definição 4. *Definimos por* ***relação binária*** *de A em B todo subconjunto R de $A \times B$.*

Se $(a, b) \in R$, dizemos que *a se relaciona com b*, escrevendo de forma usual que aRb, ao longo dessa seção.

Exemplo 1. *Seja X um conjunto qualquer e seja R o conjunto de todos os pares (x,y) de $X \times X$ para os quais $x = y$. A relação R aqui estabelecida é a de igualdade entre os elementos, ou seja, x se relaciona com y, é o mesmo que $x = y$.*

Exemplo 2. *Sejam X um conjunto qualquer e R o conjunto de todos os pares (x,A) de $X \times \mathcal{P}(X)$ para os quais $x \in A$n onde $\mathcal{P}(X)$ é o conjunto das partes de X. A relação R é tal que se $x \in X$ e $A \in \mathcal{P}(X)$, então xRA é o mesmo que $x \in A$.*

Definição 5. *Seja X um conjunto não vazio. Dizemos que uma relação R é:*

i) ***reflexiva****, se xRx para todo $x \in X$;*

ii) ***simétrica****, se xRy implicar yRx, para todos $x, y \in X$;*

iii) ***transitiva****, se xRy e yRz implicar xRz para todos x, y e $z \in X$;*

iv) ***antissimétrica****, se xRy e yRx implicar $x = y$ para todos $x, y \in X$.*

Definição 6. *Dizemos que R é uma* ***relação de equivalência*** *sobre um conjunto X se for reflexiva, simétrica e transitiva.*

Exemplo 3. *A igualdade é uma relação de equivalência. De fato, como visto no Exemplo 1 dados x, y e $z \in X$ quaisquer temos que $x = x$, isto é, xRx naturalmente. Além disso, dizer que $x = y$ é o mesmo que $y = x$, logo se xRy então yRx e portanto R é simétrica. Agora se $x = y$ e $y = z$ podemos concluir que $x = z$, e isso nos diz que como xRy e yRz então xRz. Portanto a igualdade é uma relação de equivalência.*

Exemplo 4. *Dado X um conjunto não vazio, temos que o produto cartesiano $X \times X$ define uma relação de equivalência.*

Definição 7. *Uma **ordem parcial** em um conjunto X é uma relação reflexiva, antissimétrica e transitiva.*

Exemplo 5. *Dado um conjunto X, a relação de inclusão ($\subset$) em $\mathcal{P}(X)$ é uma ordem parcial.*

Definição 8. *Um **conjunto parcialmente ordenado** é um par ordenado $(X, \leq)$ em que X é um conjunto e $''\leq''$ uma ordem parcial nele.*

Definição 9. *Seja R uma relação de ordem parcial sobre X. Dados $x, y \in X$, dizemos que x e y são **comparáveis mediante R** se $x \leq y$ ou $y \leq x$. Caso contrário, dizemos que são não comparáveis.*

Definição 10. *Se dois elementos quaisquer de um conjunto X forem comparáveis mediante R, então R é dito **relação de ordem total** sobre X. Nesse caso, X é chamado de **conjunto totalmente ordenado**.*

Exemplo 6. *A ordem parcial em qualquer conjunto X de números reais (com a ordem natural) é uma ordem total, uma vez que dois números reais quaisquer são sempre comparáveis.*

Observação 2. *Seja X um conjunto parcialmente ordenado. Então a ordem parcial de X induz uma ordem parcial em todo subconjunto de X.*

Definição 11. *Se X é um conjunto parcialmente ordenado e A um subconjunto não vazio de X, um elemento $L \in X$ é um **limite superior** de A se, para todo $x \in A$ temos que $x \leq L$. Por outro lado dizemos que um elemento $l \in X$ é um **limite inferior** de A se para todo $x \in A$ temos que $l \leq x$.*

Definição 12. *No conjunto dos números naturais definimos $a \mid b$, ordem parcial dita **divisibilidade** para todos $a, b \in \mathbb{N}$, o que significa, $a \mid b$ se existe $c \in \mathbb{N}$ tal que $b = ac$.*

Exemplo 7. *Seja R a relação definida nos naturais como $R = \{x, y \in \mathbb{N} \mid x \text{ múltiplo de } y\}$, então temos que R é uma relação de ordem parcial.*

Exemplo 8. *Sejam $X = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $A = \{2, 4, 6\} \subseteq X$ e a ordem parcial divisibilidade. Então temos que 12 e 36 são limites superiores para A e 1 e 2 são limites inferiores.*

Definição 13. *Sejam X um conjunto parcialmente ordenado e A um subconjunto não vazio de X. Um elemento M de A é* ***máximo*** *se M é um limite superior de A. De forma análoga, um elemento m de A é* ***mínimo*** *se m é um limite inferior de A.*

Exemplo 9. *O conjunto $C = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ com a ordem de divisibilidade, temos que C não possui máximo porém possui o 1 como elemento mínimo.*

Exemplo 10. *Sejam $X = \{a, b, c\}$ e $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ o conjunto das partes de X. Como o conjunto $\emptyset$ é subconjunto de todo conjunto, ele é o elemento mínimo de $\mathcal{P}(X)$ com a relação do Exemplo 5 e X é o elemento máximo, pois todo conjunto de $\mathcal{P}(X)$ está contido nele.*

Definição 14. *Se X é um conjunto parcialmente ordenado e A um subconjunto não vazio de X, dizemos que um elemento $M \in A$ é um* ***elemento maximal*** *de A se para todo $x \in A$ de modo que $M \leq x$, então $x = M$. De forma análoga, um elemento $m \in A$ é um* ***elemento minimal*** *de A se para todo $x \in A$ de modo que $x \leq m$, então $x = m$.*

Exemplo 11. *Seja $\mathcal{C}$ a coleção de subconjuntos não vazios de um conjunto X não vazio, ordenado pela inclusão. Cada conjunto unitário é um elemento minimal de $\mathcal{C}$, porém o mesmo não possui mínimo.*

Exemplo 12. *Sejam $X = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $A = \{2, 4, 6\} \subseteq X$ e a ordem parcial divisibilidade. Temos que 2 é o elemento minimal de A e 4 e 6 são os elementos maximais de A.*

Notemos que dizer que um elemento é *máximo* ou *mínimo* dentro de um conjunto é dizer que esse elemento é comparável a todos os elementos do conjunto, diferentemente de um elemento ser *minimal* ou *maximal* no conjunto, é que não existe nenhum elemento estritamente menor ou maior do que esse elemento.

As definições a seguir possuem grande relevância para o desenvolvimento do capítulo 3.

Definição 15 (Cadeia)**.** *Definimos uma* ***cadeia*** *como sendo qualquer subconjunto $\mathcal{C}$ totalmente ordenado de um conjunto parcialmente ordenado.*

Segundo CONRAD, em um conjunto X parcialmente ordenado, podemos falar de elementos minimais tanto quanto de elementos maximais. O Lema de Zorn não é intuitivo,

mas é logicamente equivalente a declarações mais intuitivamente plausíveis na teoria dos conjuntos, como o Axioma da Escolha, afirma que todo produto cartesiano de conjuntos não vazios é não vazio.

Lema 1 (Lema de Zorn)**.** *Se X é um conjunto não vazio parcialmente ordenado tal que toda cadeia em X é limitada, então X contém um elemento maximal.*

Uma vez que nosso objetivo principal referente ao Lema de Zorn é a sua aplicação, caso seja do interesse, a demonstração da equivalência desses resultados pode ser vista em (HALMOS, 1970, página 69).

Exemplo 13. *Note que $\mathbb{Z}_+$ não é totalmente ordenado com relação a ordem divisibilidade, uma vez que a maioria dos pares de inteiros não são comparáveis sob essa relação. Por exemplo, $3 \nmid 5$ e $5 \nmid 7$.*

Exemplo 14. *O subconjunto dos inteiros, $X = \{1, 2, 4, 8, 16, ...\}$ formado pelas potências de 2 é totalmente ordenado sob a relação de divisibilidade.*

Definição 16. *Seja A um conjunto não vazio parcialmente ordenado. Uma sequência $(a_n)_{n\in\mathbb{N}}$ de elementos de A é dita uma **cadeia ascendente** (crescente) se para todo $n \in \mathbb{N}$ tem-se que $a_n \leqslant a_{n+1}$. Isto é,*

$$a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n \leqslant a_{n+1} \leqslant \ldots.$$

Definição 17. *Um **limitante superior** para uma sequência $(a_n)_{n\in\mathbb{N}}$ de elementos de A é um elemento $x \in A$ tal que $a_n \leqslant x$, para todo $n \in \mathbb{N}$. Analogamente, dizemos que um **limitante inferior** para uma sequência $(a_n)_{n\in\mathbb{N}}$ de elementos de A é um elemento $x \in A$ tal que $x \leqslant a_n$, para todo $n \in \mathbb{N}$.*

Exemplo 15. *Se $A = \mathbb{R}$ e $X =]0, 1]$ com a ordem habitual dos números reais, temos que os limitantes superiores de A são todos $x \geqslant 1$ com $x \in \mathbb{R}$.*

Exemplo 16. *Se $A = \mathbb{R}$ e $X =]2, 5]$ com a ordem habitual dos números reais, temos que os limitantes inferiores de A são todos $x \leqslant 2$ com $x \in \mathbb{R}$.*

Definição 18. *Uma sequência $(a_n)_{n\in\mathbb{N}}$ de elementos de A é dita **estacionária** se existir $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$ tivermos que $a_n = a_{n_0}$.*

Definição 19. *Dizemos que A satisfaz a **condição de cadeia ascendente (C.C.A)** se toda cadeia ascendente em A for estacionária.*

1.2 Teoria de Aneis

Os livros didáticos de álgebra geralmente dão a definição de um anel primeiro e seguem com exemplos. É claro que os exemplos vieram primeiro, e a definição abstrata depois; muito depois (KLEINER, 2007).

Na presente seção definiremos um anel como sendo comutativo com unidade e ainda, traremos alguns resultados que serão importantes para o desenvolvimento desta monografia tais como homomorfismo de aneis, elementos notáveis de um anel além das definições de domínio de integridade e corpo.

Definição 20 (Aneis)**.** *Seja A um conjunto não vazio munido das operações binárias $(+)$ e $(\cdot)$ ditas respectivamente adição e multiplicação. Dizemos que $(A,+,\cdot)$ é um* ***anel*** *se para todos $a, b, c \in A$ tivermos que:*

i) $a + (b + c) = (a + b) + c$ (associativa da adição);

ii) $a + b = b + a$ (comutativa da adição);

iii) Existe único $0 \in A$ de modo que, $a + 0 = 0 + a = a$ (neutro aditivo);

iv) Para todo $a \in A$, existe único $-a \in A$ tal que $a + (-a) = (-a) + a = 0$ (simétrico aditivo);

v) $a(bc) = (ab)c$ (associativa da multiplicação);

vi) $ab = ba$ (comutativa da multiplicação);

vii) Existe único $1 \in A$ de modo que $1a = a$ (neutro multiplicativo);

viii) A multiplicação é distributiva em relação a adição

$$a(b + c) = ab + ac \text{ e } (a + b)c = ac + bc.$$

Exemplo 17. *Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com as operações usuais são aneis.*

Exemplo 18 (Anel de funções)**.** *Seja X um conjunto não vazio. Então o conjunto*

$$A = \{f : X \longrightarrow \mathbb{R} \mid f \textit{ contínua}\}$$

munido com as operações usuais de soma e produto de funções

$$+ : (f+g)(x) = f(x) + g(x)$$
$$\cdot : (fg)(x) = f(x)g(x)$$

para todo $x \in X$, é um anel.

De fato, dados $x \in X$ e $f, g, h \in A$ temos

i) $(f + (g + h))(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = ((f + g) + h)(x)$ portanto vale a associatividade da adição.

ii) $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$ portanto vale a comutatividade da adição.

iii) Dado $f \in A$, seja $q \in A$, tal que $(f + g)(x) = 0$. Então

$$\begin{aligned}(f+q)(x) = 0 &\Leftrightarrow f(x) + q(x) = 0\\ &\Leftrightarrow f(x) + (-f(x)) + q(x) = 0 + (-f(x))\\ &\Leftrightarrow f(x) + (-f(x)) + q(x) = -f(x)\\ &\Leftrightarrow q(x) = -f(x).\end{aligned}$$

Portanto, existe $q(x) \in A$, simétrico aditivo e denotado por $-f(x)$.

iv) Existe a função nula tal que para toda $f \in A$ tem-se

$$0 + f(x) = f(x) + 0 = f(x).$$

Além disso, dados $f, g, h \in A$ temos

v) $(f(gh))(x) = f(x)(g(x)h(x)) = (f(x)g(x))h(x) = ((fg)h)(x)$. Portanto a multiplicação é associativa.

vi) $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$. Portanto a multiplicação é comutativa.

vii) $(f(g + h))(x) = (f(x)(g(x) + h(x))) = f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x)$. Portanto vale a distributiva da multiplicação em relação a adição. A outra forma é análoga.

viii) Existe a função identidade $f(x) = 1 \in A$ tal que para toda $g(x) \in A$ tem-se

$$g(x)f(x) = f(x)g(x) = g(x).$$

Proposição 2. *Sejam A um anel e $a, b, c \in A$. Se $a + b = a + c$, então $b = c$ (lei do cancelamento da adição).*

Demonstração. Se $a, b, c \in A$ tais que $a + b = a + c$ temos que

$$(-a) + (a + b) = (-a) + (a + c) \Rightarrow (-a + a) + b = (-a + a) + c \Rightarrow 0 + b = 0 + c \Rightarrow b = c.$$

□

Proposição 3. *Seja A um anel. Então para todos a, b e $c \in A$ temos:*

i) $a0 = 0$;

ii) $a(-b) = (-a)b = -(ab)$;

iii) $(-a)(-b) = ab$.

Demonstração. *i)* Note que

$$0 + a0 = a0 = a(0 + 0) = a0 + a0.$$

Aplicando a Proposição 2 tem-se que $0 = a0$.

ii) Temos, por *i)* que

$$ab + [-(ab)] = 0 = a0 = a\,[b + (-b)] = ab + a(-b).$$

Aplicando novamente a Proposição 2 temos $-(ab) = a(-b)$.

iii) Aplicando *ii)*, temos

$$(-a)(-b) = -(a(-b)) = a(-(-b)) = ab.$$

□

Exemplo 19. *Seja $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, $n \geq 0$, o conjunto das classes residuais módulo n, com as operações em $\mathbb{Z}_n$ definidas por:*

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a}\overline{b} = \overline{ab}$$

para todos $\overline{a}, \overline{b} \in \mathbb{Z}_n$. *O anel* $(\mathbb{Z}_n, +, \cdot)$ *é chamado de anel dos inteiros módulo n.*

Observação 3. *Para todo* $\overline{a}, \overline{b} \in \mathbb{Z}_n$ *temos que:*

$$\overline{a} = \overline{b} \iff a \equiv b \; mod \; n \iff n \mid (a-b).$$

Exemplo 20 (Anel de polinômios)**.** *Sejam* $A = \mathbb{Z}, \mathbb{Q}$ *ou* $\mathbb{R}$. *Então denotamos* $A[X]$ *conjunto dos polinômios na variável x com coeficientes em A, isto é,*

$$A[X] = \left\{ a_i x^i + a_{i-1} x^{i-1} + \cdots + a_1 x + a_0 \;\mid\; a_i \in A, i \in \mathbb{N} \right\} \cup \{0\}.$$

Dados $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ *e* $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$, *para todo* $m, n \in \mathbb{N} \cup \{0\}$ *com* $m \leq n$ *temos que* $A[X]$ *munido com as operações de adição e produto definidas como*

$$+ : f(x) + g(x) = \sum_{i=1}^{n} (a_i + b_i) x^i$$
$$\cdot : f(x) g(x) = \sum_{i=1}^{n+m} c_k x^k$$

em que

$$c_k = \sum_{k=1}^{m+n} a_j b_{k-j}$$

para todo $k = 0, 1, \ldots, n+m$, *é um anel.*

Definição 21. *Seja A um anel,* $a \in A$ *e* $n \in \mathbb{N} \cup \{0\}$. *Definimos*

$$a^n = \begin{cases} 1\,, & se\ n = 0 \\ a\,, & se\ n = 1 \\ a^{n-1} \cdot a\,, & se\ n > 1. \end{cases}$$

Proposição 4. *Seja A um anel em que* $a \in A$ *e* $m, n \in \mathbb{N} \cup \{0\}$. *Então*

i) $a^m a^n = a^{m+n}$;

ii) $(a^m)^n = (a)^{mn}$;

iii) $(ab)^n = a^n b^n$.

Demonstração. Façamos a demonstração por indução sobre n.

i) Se $n = 0$, então

$$a^m a^0 = a^m 1 = a^m = a^{m+0}.$$

Logo, vale a igualdade. Seja $0 \leq k \in \mathbb{N}$ e suponhamos $a^m a^k = a^{m+k}$.

Desse modo,

$$(a^m)^{k+1} = a^m(a^k a) = (a^m a^k)a = (a^{m+k})a = a^{(m+k)+1} = a^{m+(k+1)}.$$

Como a validade para $k \geq 0$ implica na validade para $k+1$, portanto vale para todo $n \geq 0$.

ii) Novamente se $n = 0$, vale a igualdade, pois

$$(a^m)^0 = a^{m \cdot 0} = a^0 = 1.$$

Agora suponhamos que para $0 \leq k \in \mathbb{N}$ temos $(a^m)^k = a^{mk}$. Daí,

$$(a^m)^k a^m = (a^{mk})a^m = a^{mk+m} = a^{m(k+1)}.$$

Como a validade para $k \geq 0$ implica na validade para $k+1$, portanto vale para todo $n \geq 0$.

iii) O caso para $n = 0$ é trivial e para $n = 1$ temos

$$(ab)^1 = ab = a^1 b^1.$$

Suponhamos válido para $0 \leq k \in \mathbb{N}$, isto é, $(ab)^k = a^k b^k$. Então temos

$$(ab)^{k+1} = (ab)^k(ab) = a^k b^k(ab) = a^k b^k ab = a^k a b^k b = a^{k+1} b^{k+1}.$$

Desse modo, vale para $k+1$, e portanto vale para todo $n \geq 0$.

□

As definições e resultados a seguir são referentes a elementos notáveis dentro de um anel e introduzimos também a noção de domínio.

Definição 22. *Se A é um anel, então um elemento $a \in A$ não nulo é dito* ***divisor de zero*** *se existir $0 \neq b \in A$ tal que $ab = 0$. Caso contrário, a é dito* ***regular****.*

Definição 23. *Sejam A um anel e $a \in A$ um elemento não nulo. Dizemos que a é* ***nilpotente****, se existir $n \in \mathbb{N}$ tal que $a^n = 0$.*

$$\text{Notação: } Nilp(A) = \{a \in A \mid a^n = 0 \text{ para algum } n \in \mathbb{N}\}.$$

Definição 24. *Dado um anel A, um elemento $u \in A$ é dito* ***invertível*** *se existe $v \in A$ tal que*

$$uv = 1,$$

em que v é chamado de ***inverso (multiplicativo)*** *de u e é usualmente denotado por u^{-1}.*

Observação 4. *Um elemento do anel é sempre associado de si mesmo.*

Definição 25. *Dois elementos $a, b \in A$, A anel, são ditos* ***associados*** *se existir um elemento invertível u de A tal que*

$$a = ub.$$

Definição 26. *Um elemento não nulo e não invertível de um anel A é dito* ***irredutível*** *se seus únicos divisores são os elementos invertíveis do anel e seu associados.*

Exemplo 21. *O número $2 \in \mathbb{Z}$ é irredutível, pois seus únicos divisores são ± 1 e ± 2.*

Proposição 5. *Um elemento nilpotente não nulo de um anel não pode ser invertível.*

Demonstração. Sejam a invertível e suponhamos que a seja nilpotente, isto é, $a^n = 0$ para algum $n \in \mathbb{N}$. Como a é invertível, existe $b \in A$ tal que

$$\begin{aligned} ab = 1 &\Rightarrow a^{n-1}(ab) = a^{n-1} \\ &\Rightarrow (a^{n-1}a)b = a^{n-1} \\ &\Rightarrow a^n b = a^{n-1} \\ &\Rightarrow 0b = a^{n-1} \\ &\Rightarrow 0 = a^{n-1}. \end{aligned}$$

Continuando o processo acima, temos que $a^{n-1} = 0$ implica que $a^{n-2} = 0$ e assim por diante, até que $a^2 = 0$ implicar que $a = 0$. Disso, obtemos que $1 = ab = 0b = 0$, absurdo. □

Definição 27. *Um elemento p não nulo e não invertível de um anel A é dito* ***primo*** *se dados $a, b \in A$, com $p \mid ab$ tivermos $p \mid a$ ou $p \mid b$.*

Exemplo 22. *O número 2 é primo em $\mathbb{Z}$, pois dados $a, b \in \mathbb{Z}$ se $2 \mid ab$ então a ou b tem que ser par.*

Definição 28 (Domínio de integridade)**.** *Se A é um anel, dizemos que A é um* ***domínio de integridade*** *se A não possuir divisores de zero.*

Proposição 6 (Lei do cancelamento)**.** *Seja A um domínio de integridade. Para todos $a, x, y \in A$ com a não nulo, se $ax = ay$ então $x = y$.*

Demonstração. Como A é domínio, em particular anel, temos que para todo $a \in A$, existe $-a \in A$. Sendo $ax \in A$, então existe $-(ax) \in A$. Então aplicando o item $iv)$ da Definição 20 e o item $ii)$ da Proposição 3 temos:

$$ax = ay \Rightarrow ax + (-(ax)) = ay + (-(ax)) \Rightarrow 0 = a(y - x).$$

Uma vez que A é domínio de integridade, devemos ter $a = 0$ ou $y - x = 0$. Como, por hipótese, a é não nulo, temos $y - x = 0$, o que implica que $y = x$. □

Exemplo 23. *O anel dos inteiros $\mathbb{Z}$ é um domínio de integridade.*

Exemplo 24. *Em $\mathbb{Z}_6$, os elementos $\overline{2}$ e $\overline{3}$ são divisores de zero, pois ambos são diferentes de zero e, $\overline{2} \cdot \overline{3} = \overline{0}$, o que prova que $\mathbb{Z}_6$ não é um domínio de integridade.*

Proposição 7. *Se A é um domínio de integridade, então $A[X]$ é domínio de integridade.*

Demonstração. Sejam $f(x), g(x) \in A[X]$ dois polinômios não nulos em que $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ e $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ com $a_n, b_m \neq 0$. Então temos,

$$f(x)g(x) = a_n b_m x^{m+n} + \cdots + a_0 b_0 \neq 0,$$

uma vez que $a_n b_m \neq 0$. □

Definição 29 (Corpo)**.** *Um anel K é dito* ***corpo*** *se todo elemento não nulo de K admite inverso multiplicativo.*

Observação 5. *Denotaremos um corpo qualquer por $\mathbb{K}$.*

Exemplo 25. *Os anéis $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos porém o anel dos inteiros $\mathbb{Z}$ não é corpo. Basta notarmos que para todo $a \in \mathbb{Z}$ não existe $\frac{1}{a} \notin \mathbb{Z}$ em que $\frac{1}{a}a = 1$.*

Proposição 8. *Todo corpo é domínio de integridade.*

Demonstração. Sejam $a, b \in \mathbb{K}$ tais que $ab = 0$ com $a \neq 0$. Como $\mathbb{K}$ é corpo, existe $a^{-1} \in \mathbb{K}$ de modo que $a^{-1}a = 1$. Daí,

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow b = 0.$$

Portanto $\mathbb{K}$ é domínio de integridade. □

Observação 6. *A recíproca da Proposição 8 é falsa. De fato, o anel dos inteiros $\mathbb{Z}$ é um domínio de integridade que não é corpo.*

A proposição a seguir estabelece uma condição para que um domínio de integridade seja corpo.

Proposição 9. *Todo domínio de integridade finito é corpo.*

Demonstração. Seja $\mathbb{K} = \{a_1, a_2, a_3, \ldots, a_n\}$ um domínio de integridade com n elementos distintos, em que para cada $a \in \mathbb{K}$ não nulo, mostraremos que a é invertível. Se $0 \neq a \in \mathbb{K}$ qualquer, tem-se que $a\mathbb{K} = \{aa_1, aa_2, \ldots, aa_n\}$. Se dados $i, j \in \{1, \cdots, n\}$ com $n \in \mathbb{N}$, temos $aa_i = aa_j$, como $\mathbb{K}$ é domínio de integridade, então, $a_i = a_j$ pela lei do cancelamento. Por hipótese $\mathbb{K}$ é finito, então obtemos $a\mathbb{K} = \mathbb{K}$, ou seja, qualquer a_i pode ser expresso como um aa_j para algum j. Em particular temos que $1 = aa_j$ para algum j, isto é, $a_j = a^{-1}$. Portanto, $\mathbb{K}$ é corpo. □

Proposição 10. *O anel $\mathbb{Z}_n$ é domínio de integridade se, e somente se n é primo. Nesse caso, $\mathbb{Z}_n$ é corpo.*

Demonstração. De fato, se $1 < n \in \mathbb{N}$ é composto, então existem $a, b \in \mathbb{Z}$ tais que $0 < a, b < n$ e $n = ab$. Portanto, temos $\overline{a}, \overline{b} \in \mathbb{Z}_n$ ambos não nulos, de modo que

$$\overline{a}\overline{b} = \overline{ab} = \overline{n} = \overline{0}.$$

Assim, $\overline{a}, \overline{b}$ são divisores de zero em $\mathbb{Z}_n$, o que prova que $\mathbb{Z}_n$ não é domínio de integridade. Reciprocamente, sejam n primo e $\overline{a}, \overline{b} \in \mathbb{Z}_n$ tais que $\overline{a}\overline{b} = \overline{ab} = \overline{0}$. Então existem $a, b \in \mathbb{Z}$ tais que $ab = nt$ em que $t \in \mathbb{Z}$, ou seja, $n \mid ab$.

Como por hipótese n é primo, então $n \mid a$ ou $n \mid b$, isto é, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Logo, $\mathbb{Z}_n$ não possui divisores próprios de $\overline{0}$ e portanto $\mathbb{Z}_n$ é domínio de integridade. Notemos que pela Proposição 9 garantimos que $\mathbb{Z}_n$ com n primo é corpo. □

Definição 30 (Homomorfismo)**.** *Dados A,B dois aneis, uma função $f : A \to B$ é dita* ***homomorfismo*** *se dados $a, b \in A$ valerem as seguintes igualdades:*

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a)f(b)$

Exemplo 26. *A função nula é um homomorfismo chamado* ***homomorfismo nulo****. De fato,*

$$f : A \longrightarrow B$$
$$f(a) = 0$$

para todo $a \in A$. Assim, dados $a, b \in A$ temos

$$f(a+b) = 0 = 0 + 0 = f(a) + f(b)$$

e

$$f(ab) = 0 = 0 \cdot 0 = f(a)f(b).$$

Exemplo 27. *Se A é um anel qualquer a função identidade*

$$f : A \longrightarrow A$$
$$f(a) = a$$

é um homomorfismo para todo $a \in A$, dito ***homomorfismo identidade.***

$$f(a+b) = a + b = f(a) + f(b)$$

e,

$$f(ab) = a \cdot b = f(a)f(b).$$

Proposição 11. *Se $f : A \longrightarrow B$ é um homomorfismo de anéis, então:*

i) f(0) = 0;

ii) $f(-a) = -f(a)$;

iii) Se f é bijetora, então $f^{-1} : A \longrightarrow B$ é um homomorfismo de aneis.

Demonstração. *i)* Sabemos que

$$0 = 0 + 0.$$

Aplicando f em ambos os lados da equação acima e usando o fato de f ser homomorfismo, temos

$$f(0) = f(0 + 0) = f(0) + f(0).$$

Somando $-f(0)$, obtemos $f(0) = 0$.

ii) Note que

$$0 = f(0) = f(a + (-a)) = f(a) + f(-a).$$

Daí, $0 = f(a) + f(-a)$, ou seja, $-f(a) = f(-a)$.

iii) Se f é bijetora, então dados $y, y^{'} \in B$ existem únicos $x, x^{'} \in A$ tais que $f(x) = y$ e $f(x^{'}) = y^{'}$.

Daí,

$$f^{-1}(y + y') = f^{-1}(f(x) + f(x')) = f^{-1}(f(x + x')) = x + x' = f^{-1}(y) + f^{-1}(y').$$

Além disso,

$$f^{-1}(y \cdot y') = f^{-1}(f(x) \cdot f(x')) = f^{-1}(f(x \cdot x')) = x \cdot x' = f^{-1}(y) \cdot f^{-1}(y').$$

Portanto f^{-1} é um homomorfismo de anéis.

□

Se um homomorfismo é uma função sobrejetora, ele é dito um **homomorfismo sobrejetor** ou **epimorfismo**. Se um homomorfismo é uma função injetora, ele é dito um **homomorfismo injetor** ou **monomorfismo**.

Definição 31 (Núcleo)**.** *Dado um homomorfismo de anéis $f : A \longrightarrow B$, o **núcleo** de f é o subconjunto $Ker(f) \subset A$ tal que*

$$Ker(f) = \{x \in A \mid f(x) = 0_B\}.$$

Proposição 12. *Seja $f : A \longrightarrow B$ um homomorfismo sobrejetor de anéis. Então temos que:*

i) O elemento $f(1_A)$ é a unidade do anel B;

ii) Se $a \in A$ é invertível, então $f(a)$ também o é, ou seja, $(f(a))^{-1} = f(a^{-1})$.

A demonstração desta proposição pode ser consultada em (DOMINGUES; IEZZI, 2003, página 234).

1.3 Teoria de Ideais

Segundo HEFEZ, a definição de ideal foi introduzida no final do século dezenove por Kummer e Dedekind a fim de estudar certas questões em Teoria dos Números. Essa noção tornou-se um objeto central na teoria dos aneis.

Na presente seção, apresentaremos as definições de ideais de um anel A, ideais finitamente gerados, além de algumas propriedades operacionais. Por fim traremos o conceito de anel quocientado por um ideal I.

Definição 32 (Ideal)**.** *Seja I um subconjunto não vazio de um anel A. Dizemos que I é um **ideal** de A se para todos $a, b \in I$ e $r \in A$:*

i) $a - b \in I$;

ii) $ar \in I$.

Exemplo 28. *Em todo anel A, temos que $I = \{0\}$ e o próprio A são ideais ditos os **ideais triviais**.*

Definição 33. *Dizemos que A é um **anel simples** se possuir apenas os ideais triviais.*

Definição 34. *Se A é um anel, então todo ideal $I \subset A$ tal que $I \neq A$ é dito **ideal próprio**.*

Exemplo 29. *Para qualquer inteiro n positivo temos que o conjunto $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.*

De fato, $n\mathbb{Z} \neq \emptyset$, pois $0 \in n\mathbb{Z}$. Além disso, dados $a, b \in n\mathbb{Z}$, temos que $a = tn$ e $b = sn$ com t e s inteiros. Assim,

$$a - b = tn - sn = (t - s)n = qn \in n\mathbb{Z}.$$

E ainda, dado $r \in \mathbb{Z}$, temos

$$ar = (tn)r = (tr)n \in n\mathbb{Z}.$$

Portanto, $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$.

Proposição 13. *Sejam A um anel e I um ideal de A. Se I possui um elemento invertível de A, então $I = A$.*

Demonstração. Sendo I um ideal de A, temos que $I \subseteq A$. Por outro lado, dados $a \in A$ e $x \in I$ um elemento invertível de A, por hipótese, existe $x^{-1} \in A$. Como I é ideal, temos que $a = (ax^{-1})x \in I$ e portanto $A \subseteq I$. □

Exemplo 30. *Um corpo só possui os ideais triviais. De fato, se I é um ideal do corpo $\mathbb{K}$ de modo que $I \neq \{0\}$, então existe $0 \neq a \in I$ em que $a \in \mathbb{K}$, pois $I \subseteq \mathbb{K}$. Sendo $\mathbb{K}$ corpo, existe $a^{-1} \in \mathbb{K}$ e ainda, pela Proposição 13, I possui elemento invertível. Portanto, $I = \mathbb{K}$. Logo, $\mathbb{K}$ só possui os ideais triviais.*

Proposição 14. *Sejam I e J ideais de um anel A. Então:*

i) $I \cap J = \{x \in A \mid x \in I \text{ e } x \in J\}$ *é um ideal de A;*

ii) $I + J = \{x + y \in A \mid x \in I \text{ e } y \in J\}$ *é um ideal de A;*

iii) $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \;\mid\; a_i \in I \text{ e } b_i \in J \text{ e } n \in \mathbb{N} \right\}$ *é um ideal de A;*

iv) $IJ \subseteq I \cap J$.

Demonstração. *i)* Temos que $I \cap J \neq \emptyset$ pois como I e J são ideais então $0 \in I$ e $0 \in J$, donde $0 \in I \cap J$. Além disso, se $x, y \in I \cap J$, então $x, y \in I$ e $x, y \in J$. Daí $x - y \in I$ e $x - y \in J$, ou seja, $x - y \in I \cap J$. Agora se $r \in A$, então temos que $xr \in I$ e $xr \in J$ uma vez que ambos são ideais. Logo, $xr \in I \cap J$. Portanto, $I \cap J$ é ideal de A.

ii) Note que $I + J \neq \emptyset$ pois como I e J são ideais temos que $0 \in I$ e $0 \in J$ e portanto $0 = 0 + 0 \in I + J$. Se $x, y \in I + J$ então temos que existem $i_1, i_2 \in I$ e $j_1, j_2 \in J$ tais que $x = i_1 + j_1$ e $y = i_2 + j_2$.

Assim,

$$x - y = (i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J.$$

Ainda, dado $r \in A$, obtemos

$$xr = (i_1 + j_1)r = i_1 r + j_1 r \in I + J.$$

Portanto, $I + J$ é ideal de A.

iii) Temos que $IJ \neq \emptyset$, pois como $0 \in I$ e $0 \in J$ então $0 \in IJ$. Sejam $x, y \in IJ$, então $x = \sum_{i=1}^{n} a_i b_i$ e $y = \sum_{j=1}^{m} c_j d_j$ com $a_i, c_j \in I$ e $b_i, d_j \in J$. Como I é ideal, temos que $(-c_j) \in I$ e assim,

$$x - y = \sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} c_j d_j = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} (-c_j) d_j,$$

que é soma finita de elementos de I multiplicados por elementos de J, ou seja, $x - y \in IJ$.

E ainda, dado $r \in A$ e $a_i \in I$, obtemos

$$rx = r \sum_{i=1}^{n} a_i b_i = x = \sum_{i=1}^{n} (r a_i) b_i \in IJ.$$

Portanto, IJ é ideal A.

iv) Dado $x \in IJ$, temos $x = \sum_{i=1}^{n} a_i b_i$ em que $a_i \in I$ e $b_i \in J$. Como $J \subseteq A$, temos que para todo $b_i \in J$, então $b_i \in A$ e daí $x \in I$, o que implica que $IJ \subseteq I$. De forma análoga, para todo $a_i \in I$ temos que $a_i \in A$, ou seja, $x \in J$ e com isso $IJ \subseteq J$. Portanto $IJ \subseteq I \cap J$.

□

Observação 7. *Dados I e J ideais de um anel A, temos que $I \cup J$ nem sempre é ideal de A. A título de ilustração, considere $2\mathbb{Z} \cup 3\mathbb{Z} = \{x \in \mathbb{Z} \mid 2 \mid x \text{ ou } 3 \mid x\}$. Note que $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, porém $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Uma condição para que a união de ideais seja um ideal é dada no item ii) da Proposição 16.*

Proposição 15. *Seja $f : A \longrightarrow B$ um homomorfismo de anéis. Se J é um ideal de B, então*

$$f^{-1}(J) = \{x \in A \mid f(x) \in B\}$$

é um ideal de A.

Demonstração. Como $f(0_A) = 0_B \in J$ então $0_A \in f^{-1}(J)$ e assim $f^{-1}(J) \neq \emptyset$. Além disso, se $x, y \in f^{-1}(J)$ temos $f(x), f(y) \in J$ e sendo J ideal de B, temos $f(x) - f(y) = f(x-y) \in J$, ou seja, $x - y \in f^{-1}(J)$. Seja $\alpha \in A$ e $x \in f^{-1}(J)$. Então $f(x) \in J$. Mas como J é um ideal de B, temos $f(\alpha \cdot x) = f(\alpha) \cdot f(x) \in J$, ou seja, $\alpha \cdot x \in f^{-1}(J)$. Portanto, $f^{-1}(J)$ é ideal de A. □

Proposição 16. *Se $\{I_i\}_{i\in\mathbb{N}}$ é uma família de ideais de A, então:*

i) $\bigcap_{i\in\mathbb{N}} I_i$ *é um ideal de A;*

ii) se $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$, então $I = \bigcup_{i\in\mathbb{N}} I_i$ é ideal de A.

Demonstração. *i)* Sejam $\{I_i\}_{i\in\mathbb{N}}$ uma família de ideais com $x, y \in \bigcap_{i\in\mathbb{N}} I_i$ e $a \in A$. Então para todo $i \in \mathbb{N}$ temos que $x - y \in I_i$ e $ax \in I_i$, uma vez que cada I_i é um ideal de A e, portanto, temos que $x - y \in \bigcap_{i=1}^{n} I_i$ e $ax \in \bigcap_{i=1}^{n} I_i$.

ii) Se $x, y \in I$ então existem $m, n \in \mathbb{N}$ tais que $x \in I_m$ e $y \in I_n$. Tomando $r = máx\{m, n\}$ temos que $x, y \in I_r$ e consequentemente $x - y \in I$. De modo similar, temos que $x \in I$ e $a \in A$ temos que $xa \in I$ e, portanto, $I = \bigcup_{i\in\mathbb{N}} I_i$ é ideal de A.

□

Sejam $a_1, a_2, \cdots, a_n$ elementos de um anel A e consideremos o subconjunto a seguir:

$$\langle a_1, a_2, \cdots, a_n\rangle = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_1, x_2, \cdots, x_n \in A\} \tag{1.1}$$

com $n \in \mathbb{N}$.

Proposição 17. *O conjunto definido em (1.1) é um ideal de A.*

Demonstração. Note que $\langle a_1, a_2, \cdots, a_n\rangle \neq \emptyset$, pois $0 \in \langle a_1, a_2, \cdots, a_n\rangle$ uma vez que $0 = a_10 + a_20 + \cdots + a_n0$. E ainda, dados $r, s \in \langle a_1, \cdots, a_n\rangle$ existem $x_1, \cdots, x_n$ e $y_1, \cdots, y_n$

elementos de A tais que $r = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ e $s = a_1y_1 + a_2y_2 + \cdots + a_ny_n$. Assim,

$$\begin{aligned} r - s &= (a_1x_1 + a_2x_2 + \cdots + a_nx_n) - (a_1y_1 + a_2y_2 + \cdots + a_ny_n) \\ &= a_1 \underbrace{(x_1 - y_1)}_{\in A} + a_2 \underbrace{(x_2 - y_2)}_{\in A} + \cdots + a_n \underbrace{(x_n - y_n)}_{\in A} \in \langle a_1, \cdots, a_n \rangle . \end{aligned}$$

Além disso, dado $\beta \in A$ temos

$$\begin{aligned} r \cdot \beta &= (a_1x_1 + a_2x_2 + \cdots + a_nx_n)\beta \\ &= a_1 \underbrace{(x_1 \cdot \beta)}_{\in A} + a_2 \underbrace{(x_2 \cdot \beta)}_{\in A} + \cdots + a_n \underbrace{(x_n \cdot \beta)}_{\in A} \in \langle a_1, \cdots, a_n \rangle . \end{aligned}$$

Portanto $\langle a_1, \cdots, a_n \rangle$ é um ideal de A. □

Definição 35. *Se A é um anel e $S = \{a_1, a_2, a_3, \cdots, a_n\} \subset A$, então o ideal $\langle S \rangle$ é dito* ***ideal finitamente gerado*** *pelos elementos de S.*

Definição 36. *Se $a \in A$ então $\langle a \rangle = \{ax \mid x \in A\}$ é um* ***ideal principal*** *gerado por a.*

Definição 37. *Um domínio de integridade cujos ideais são todos principais é chamado de* ***Domínio de Ideais Principais (DIP).***

Exemplo 31. *O anel dos inteiros $\mathbb{Z}$ é um DIP. De fato, se J é o ideal do anel $\mathbb{Z}$ tal que $J = \langle 0 \rangle$, não há o que fazer. Supondo $J \neq \langle 0 \rangle$, então existe $0 \neq a \in J$ tal que $-a \in J$, ou seja, $|a| \in J$. Considerando $d \in \mathbb{Z}$ o menor inteiro positivo de J, queremos mostrar que $J = d\mathbb{Z}$. De fato, se $a \in d\mathbb{Z}$ então $a = dn$ para algum $n \in \mathbb{Z}$ e ainda, visto que J é ideal temos que $dn = a \in J$ e portanto, $d\mathbb{Z} \subseteq J$.*

Por outro lado, sendo $a \in J$, temos pela divisão euclidiana que existem $q, r \in \mathbb{Z}$ tais que $a = qd + r$ em que $0 \leq r < d$, ou seja, $a - qd = r$. Sendo a, $qd \in J$ e $0 \leq r < d$, temos pela minimalidade de d que $r = 0$, ou seja, $a \in d\mathbb{Z}$. Portanto $J \subseteq d\mathbb{Z}$.

Teorema 1. *Sejam $I = \langle x \rangle$ e $J = \langle y \rangle$ ideais de $\mathbb{Z}$. Temos que $I + J = \langle mdc(x, y) \rangle$ e $I \cap J = \langle mmc(x, y) \rangle$.*

A demonstração pode ser vista em (DOMINGUES; IEZZI, 2003, página 261).

Teorema 2. *Sejam $I = \langle x \rangle$ e $J = \langle y \rangle$ ideais de $\mathbb{Z}$. Então $IJ = I \cap J$ se, e somente se, I e J são coprimos entre si.*

Demonstração. Pelo item *iv*) da Proposição 14, $IJ \subseteq I \cap J$. Então basta mostrarmos que $I \cap J \subseteq IJ$. Se $z \in I \cap J$, como I e J são coprimos, então existem $x \in I$ e $y \in J$ tais que $1 = x + y$. Daí, temos que

$$z = zx + zy.$$

E assim,

$$\begin{cases} z \in J \text{ e } x \in I \\ z \in I \text{ e } y \in J \end{cases} \Rightarrow z \in IJ.$$

Portanto $I \cap J \subseteq IJ$ e, assim, concluímos a demonstração. □

Lema 2. *Seja $I_1 \subset I_2 \subset \cdots I_n \subset \cdots$ uma cadeia ascendente de ideais num domínio principal A. Então existe $m \in \mathbb{N}$ tal que $I_m = I_{m+i}$, para todo $i \geq 0$.*

Demonstração. Sejam $I = \bigcup_{i=1}^{\infty} I_i$ ideal de A e $d \in A$ de modo que $I = \langle d \rangle$. Como $d \in I$, temos que existe $m \in \mathbb{N}$ tal que $d \in I_m$, então $\langle d \rangle \subseteq I_m$ tal que $I_m \subseteq I = \langle d \rangle \subseteq I_m$. Assim, $I = I_m$ e se repetirmos o processo acima, temos que para todo $i > 0$,

$$I_m \subseteq I_{m+i} \subseteq I = I_m.$$

Ṗortanto $I_m = I_{m+i}$. □

Exemplo 32. *Sejam $A = \mathbb{Z}_{12}$ e $\langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\}$, $\langle \overline{8} \rangle = \{\overline{0}, \overline{8}\}$ ideais de $\mathbb{Z}_{12}$. Temos que $\overline{8} \in \langle \overline{4} \rangle$ e além disso $\langle \overline{8} \rangle \subseteq \langle \overline{4} \rangle$.*

Agora seja A um anel e I um ideal de A. Definamos a relação $\sim$ em A por:

$$a \sim b \Leftrightarrow a - b \in I \tag{1.2}$$

para todo $a, b \in A$.

Proposição 18. *A relação definida em (1.2) é uma relação de equivalência em A.*

Demonstração. Visto que $a - a = 0 \in I$, temos que $a \sim a$ e portanto " $\sim$ " é reflexiva. Sendo $a \sim b$ então $a - b \in I$ e daí, $b - a = -(a - b) \in I$, segue que $b \sim a$ e portanto " $\sim$ " é simétrica. Se dados $a, b, c \in A$, $a \sim b$ e $b \sim c$ então temos que $a - b \in I$ e $b - c \in I$. Desse modo, $a - c = (a - b) + (b - c) \in I$. Logo $\sim$ é transitiva e portanto " $\sim$ " é uma relação de equivalência. □

Além disso, para todo $a \in A$ denotemos $\overline{a} = a + I := \{x \in A \mid x \sim a \in I\}$. Consideremos então A/I o conjunto das **classes de equivalência de** $\sim$, isto é,

$$A/I = \{a + I \mid a \in A\}.$$

Definamos as seguintes operações em A/I :

$$+ : (a + I) + (b + I) = (a + b) + I.$$
$$\cdot : (a + I) \cdot (b + I) = (a \cdot b) + I.$$

Proposição 19. *As operações acima estão bem definidas.*

Demonstração. Se $a + I = a' + I$ e $b + I = b' + I$, então existem $x_1, x_2 \in I$ tais que $a = a' + x_1$ e $b = b' + x_2$. Desse modo,

$$\begin{aligned}(a + I) + (b + I) = (a + b) + I &= ((a' + x_1) + (b' + x_2)) + I \\ &= (a' + b') + (x_1 + x_2) + I \\ &= (a' + b') + I + \underbrace{(x_1 + x_2)}_{\in I} + I \\ &= (a' + b') + I + (0 + I) \\ &= (a' + b' + 0) + I = (a' + b') + I \\ &= (a' + I) + (b' + I).\end{aligned}$$

Além disso,

$$\begin{aligned}(a + I) \cdot (b + I) = (a \cdot b) + I &= ((a' + x_1) \cdot (b' + x_2)) + I \\ &= (a'b' + a'x_2 + x_1b' + x_1x_2) + I \\ &= (a'b' + I) + \underbrace{((a'x_2 + x_1b' + x_1x_2)}_{\in I} + I \\ &= (a'b') + I \\ &= (a' + I) \cdot (b' + I).\end{aligned}$$

□

Proposição 20 (Anel quociente)**.** *Seja I um ideal de A. Com as operações acima definidas tem-se que $(A/I, +, \cdot)$ é anel chamado* ***anel quociente*** *em que $1 + I$ é o neutro da multiplicação e $0 + I$ é o nulo de A/I.*

A demonstração desta proposição pode ser consultada em (BHATTACHARYA; JAIN; NAGPAUL, 1994, página 184).

Exemplo 33. *Sejam A um anel e I ideal de A. Temos que $a + I \in A/I$ é invertível se, e somente se, existe $r \in A$ tal que $1 - ar \in I$. De fato, se $a + I$ é invertível, então existe $r + I \in A/I$ com $r \in A$ tal que $(a + I)(r + I) = 1 + I$, ou seja,*

$$(a + I)(r + I) = 1 + I \Rightarrow ar + I = 1 + I \Rightarrow 1 - ar \in I.$$

Reciprocamente, se existe $r \in A$ tal que

$$1 - ar \in I \Rightarrow ar + I = (a + I)(r + I) = 1 + I.$$

Portanto $a + I$ é invertível em A/I.

Proposição 21. *Seja I um ideal em A e consideremos a seguinte aplicação:*

$$\pi : A \longrightarrow A/I$$
$$\pi(a) = a + I$$

para todo $a \in A$. Então π é um homomorfismo sobrejetor de anéis com o $Ker(\pi) = I$, dito ***homomorfismo projeção canônica.***

Demonstração. Dados $a, b \in A$ temos que

$$\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b)$$

e,

$$\pi(ab) = (ab) + I = (a + I)(b + I) = \pi(a)\pi(b)$$

Logo π é um homomorfismo. E ainda, se $a + I \in A/I$ como $a \in A$, temos

$$\pi(a) = a + I,$$

portanto π é sobrejetora. Além disso,

$$\begin{aligned} Ker(\pi) &= \{a \in A \mid \pi(a) = 0_B\} \\ &= \{a \in A \mid \pi(a) = a + I = 0 + I\} \\ &= \{a \in A \mid a \in I\} \\ &= I. \end{aligned}$$

□

1.4 Ideais Maximais e Primos

Existem dois tipos muito especiais de ideais: maximais e primos. No primeiro tipo, os ideais são maximais com relação a inclusão de conjuntos no anel. Já no segundo tipo, muito similar a definição de número primo sobre o conjunto dos inteiros positivos, o ideal absorve o produto de dois elementos do anel se, e somente se, um deles já está no ideal.

Na presente seção exibiremos os principais resultados relacionados a esses dois ideais.

Definição 38 (Ideal Maximal)**.** *Se A é um anel, dizemos que um ideal $M \neq A$ é um* ***ideal maximal*** *sempre que um ideal J de A é tal que se $M \subset J$, então ou $M = J$ ou $M = A$.*

Exemplo 34. *O ideal $\langle 0 \rangle$ não é maximal em $\mathbb{Z}$. Basta notarmos que $\langle 0 \rangle \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.*

Exemplo 35. *No anel $A = 2\mathbb{Z}$ o ideal $4\mathbb{Z}$ é maximal. Suponha que I seja um ideal de A tal que $4\mathbb{Z} \subseteq I \subseteq A$. Então temos que existe $m \in \mathbb{Z}$ em que $I = 2m\mathbb{Z}$ e assim $4\mathbb{Z} \subseteq 2m\mathbb{Z} \subseteq 2\mathbb{Z}$. Daí, $2m \mid 4$, ou seja, $m = 1$ ou $m = 2$. Assim, temos que $I = 2\mathbb{Z} = A$ ou $I = 4\mathbb{Z}$ e portanto $4\mathbb{Z}$ é maximal em A.*

Teorema 3. *Se A é um anel então M é um ideal maximal de A se, e somente se, A/M é corpo.*

Demonstração. Seja M um ideal maximal de A, de modo que a classe $a + M$ não seja o elemento neutro, com $a \in A$. Queremos mostrar que todo elemento $a + M$ é invertível no anel quociente. Primeiro note que $a \notin M$ e portanto $\langle a \rangle + M = A$ uma vez que o ideal $\langle a \rangle + M$ contém M propriamente. Temos que

$$1 = ab + m \Rightarrow 1 - ab = m \in M \tag{1.3}$$

para algum $b \in A$ e $m \in M$. Portanto,

$$1 + M = ab + M = (a + M)(b + M). \tag{1.4}$$

Logo, $a + M$ é invertível em A/M e portanto A/M é corpo. Reciprocamente, sendo A/M corpo, temos que $M \neq A$, caso contrário, $A/M = \{0 + M\}$ o que é uma contradição. Sejam J ideal de A de modo que $J \supsetneq M$ e um elemento $a \in J \setminus M$. Temos que $a + M \neq 0 + M$, ou seja, $a + M$ é um elemento não nulo em A/M e sendo A/M corpo, existe $b \in A$ de modo que

$$1 + M = (a + M)(b + M) = ab + M \tag{1.5}$$

e assim, $1 - ab \in M \subseteq J$. Como $a \in J$, então $1 \in J$ consequentemente temos $J = A$. □

Corolário 1. *Se A é um anel, então são equivalentes:*

i) O ideal $\langle 0 \rangle$ é maximal em A;

ii) O anel A é corpo.

Demonstração. i) $\Rightarrow$ ii) Vamos mostrar que $0 \neq a \in A$ é invertível. Se $0 \neq a \in A$, temos que $a = a1 \in aA$ implica que $\langle aA \rangle \neq \langle 0 \rangle$ e desse modo, $\langle 0 \rangle \subsetneq \langle aA \rangle \subseteq \langle A \rangle$. Uma vez que $\langle 0 \rangle$ é maximal, temos que $aA = A$, ou seja, $1 \in aA$ e portanto existe $a^{-1} \in A$ tal que $aa^{-1} = 1$, logo A é corpo.
ii) $\Rightarrow$ i) Dado I um ideal de A em que $\langle 0 \rangle \subseteq I$, se $I = \langle 0 \rangle$ não há o que fazer. Caso contrário, $I \neq \langle 0 \rangle$ e portanto existe $0 \neq a \in I \subseteq A$. Como A é corpo, existe $a^{-1} \in A$ de modo que $aa^{-1} = 1$, ou seja, I possui elemento invertível em I, e portanto $I = A$. Daí, ou $I = \langle 0 \rangle$ ou $I = A$, ou seja, o ideal $\langle 0 \rangle$ é maximal de A.

□

Exemplo 36. *Uma vez que $\mathbb{Z}$ não é corpo o ideal $\langle 0 \rangle$ não é maximal.*

Através da aplicação do Lema 1 mostraremos que de fato que os ideais maximais existem.

Teorema 4 (Krull)**.** *Todo anel não nulo contém um ideal maximal.*

Demonstração. Sejam A anel não nulo e Ω o conjunto de todos os ideais próprios de A parcialmente ordenados pela inclusão. Então temos que $\Omega \neq \emptyset$ uma vez que $\langle 0 \rangle \in \Omega$. Vamos

mostrar aplicando o Lema de Zorn, que Ω possui um elemento maximal. Seja $\mathcal{C} = \{I_\alpha\}$ uma cadeia de ideais em Ω. Então $I = \bigcup_\alpha I_\alpha$ é um ideal de A pelo item ii) da Proposição 16. Além disso, para cada par de índices α e β nesta cadeia, temos que $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$. Supondo que I não seja um ideal próprio de A, então $1 \in I$ e como $I = \bigcup_\alpha I_\alpha$, isso implica que $1 \in I_\alpha$ para algum α. O que é uma contradição com o fato de I_α ser um ideal próprio. Assim, I é uma cota superior para $\mathcal{C}$ e daí, pelo Lema de Zorn, existe $M \in \Omega$ elemento maximal. Dado K um ideal de A em que $M \subseteq K \subsetneq A$, como $K \neq A$, então $K \in \Omega$ e como M é elemento maximal em Ω, obtemos que $M = K$. Portanto, M é ideal maximal em A. □

Corolário 2. *Todo ideal próprio I de A está contido num ideal maximal.*

A demonstração desse Corolário pode ser consultada em (CONRAD, 2008, página 11).

Corolário 3. *Se A é um anel, então todo elemento de A que não é invertível está contido em um ideal maximal.*

Demonstração. Se a é um elemento não invertível de A, então temos que para todo $r \in A, ar \neq 1$ e assim, $aA \neq A$ uma vez que $1 \in A$ e $1 \notin aA$. Como aA é ideal próprio de A e $aA \neq A$ pelo Corolário 2 existe M ideal maximal de A de modo que $aA \subseteq M$. Mas isso nos diz que $a \in M$. □

Exemplo 37. *Temos que $\overline{2}$ não é invertível em $\mathbb{Z}_4$, mas pelo Corolário 2 existe M ideal maximal de $\mathbb{Z}_4$ de modo que $\overline{2} \in M$. Considerando $M = \overline{2} \cdot \mathbb{Z}_4 = \langle \overline{0}, \overline{2} \rangle$ temos que $\overline{2} \in M$ e além disso, M é maximal de $\mathbb{Z}_4$ visto que os ideais de $\mathbb{Z}_4$ são $\langle \overline{0} \rangle, \langle \overline{0}, \overline{2} \rangle$ e o próprio $\mathbb{Z}_4$.*

Definição 39 (Ideal Primo)**.** *Se A é um anel, dizemos que um ideal próprio P é um **ideal primo** de A se, para todos $a, b \in A$, sempre que $ab \in P$ tivermos que $a \in P$ ou $b \in P$.*

Exemplo 38. *Se A é um domínio de integridade, então o ideal $\langle 0 \rangle$ é um ideal primo.*

De fato, dados $a, b \in A$ tais que $ab \in \langle 0 \rangle$, então temos que $ab = 0$, isto é, ou $a = 0$ ou $b = 0$ uma vez que por hipótese A é domínio de integridade. Assim $a \in \langle 0 \rangle$ ou $b \in \langle 0 \rangle$ e, portanto $\langle 0 \rangle$ é primo.

Proposição 22. *O ideal $n\mathbb{Z}$ é primo se, e somente se, $n \in \mathbb{Z}$ é primo.*

Sejam $n\mathbb{Z}$ ideal primo e $a, b \in \mathbb{Z}$ tais que $n = ab, 1 \leqslant a, b \leqslant n$. Então devemos mostrar que $n = a$ ou $n = b$. Como $ab \in n\mathbb{Z}$, então $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$, ou seja, $n \mid a$ ou $n \mid b$. Digamos $n \mid a$, isto é, existe $q \in \mathbb{Z}$ tal que

$$a = nq = abq \Rightarrow bq = 1,$$

donde $b = 1$ e $n = a$. O caso $n \mid b$ é análogo. Reciprocamente, se $n \in n\mathbb{Z}$ é primo, ou seja, $ab \in n\mathbb{Z}$, então $n \mid ab$ implica que $n \mid a$ ou $n \mid b$. Daí, $ab \in n\mathbb{Z}$ implica que $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$, portanto $n\mathbb{Z}$ é um ideal primo.

Proposição 23. *Seja*

$$f : A \longrightarrow A/I$$
$$f(a) = a + I$$

o homomorfismo sobrejetor em que I é um ideal de A. Se $\mathcal{Q}$ é um ideal primo de A/I, então $f^{-1}(\mathcal{Q}) = P$, em que P é um ideal primo de A.

Demonstração. Temos, pelo item *iv*) da Proposição 15, que $f^{-1}(\mathcal{Q})$ é um ideal de A. Então basta mostrarmos que $f^{-1}(\mathcal{Q})$ é primo. Dados $x, y \in A$ temos que se $xy \in f^{-1}(\mathcal{Q})$, então $f(x)f(y) = f(xy) \in \mathcal{Q}$. Como $\mathcal{Q}$ é ideal primo de A/I, isso implica que $f(x) \in \mathcal{Q}$ ou $f(y) \in \mathcal{Q}$, isto é, $x \in f^{-1}(\mathcal{Q})$ ou $y \in f^{-1}(\mathcal{Q})$. Portanto $f^{-1}(\mathcal{Q})$ é ideal primo de A. □

Teorema 5. *Em um anel A, todo ideal maximal é primo.*

Demonstração. Sejam M um ideal maximal de A e $a, b \in A$ tais que $ab \in M$ com $a \notin M$ e consideremos $I = \langle a \rangle + M$. Uma vez que $1 \in A$, temos que $a = 1a + 0 \in I$, e assim, $M \subsetneq I \subseteq A$. Como M é maximal, temos que que $I = A$. Em particular, $1 \in A = \langle a \rangle + M$, e com isso, existem $m \in M$ e $x \in A$ tais que $1 = ax + m$. Isto é,

$$1 = ax + m \Rightarrow 1b = (ax + m)b = (axb) + mb = (ab)x + mb. \tag{1.6}$$

Uma vez que $ab \in M$ e $m \in M$ temos que $b \in M$. Portanto M é ideal primo de A. □

Observação 8. *A recíproca do Teorema 5 não é verdadeira. De fato, o ideal $\langle 0 \rangle \times \mathbb{Z}$ é primo em $\mathbb{Z} \times \mathbb{Z}$ mas não é maximal, pois se $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ tais que $(ac, bd) \in \langle 0 \rangle \times \mathbb{Z}$, então temos que $ac = 0$, ou seja, $a = 0$ ou $c = 0$. Mas então, $(a, b) \in \langle 0 \rangle \times \mathbb{Z}$ ou $(c, d) \in \langle 0 \rangle \times \mathbb{Z}$ e portanto $\langle 0 \rangle \times \mathbb{Z}$ é primo. Além disso, notemos que $2\mathbb{Z} \times \mathbb{Z}$ também é um ideal de $\mathbb{Z} \times \mathbb{Z}$ e que $2\mathbb{Z} \times \mathbb{Z} \supsetneq \langle 0 \rangle \times \mathbb{Z}$ e $2\mathbb{Z} \times \mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$.*

Proposição 24. *O ideal P é primo se, e somente se, A/P é um domínio de integridade.*

Demonstração. Sejam P um ideal primo de A e $(a+P),(b+P)$ pertencentes a A/P de modo que $(a+P)(b+P) = ab+P = P$, ou seja, $ab \in P$. Como P é primo, temos que $a \in P$ ou $b \in P$, isto é, $a+P = P$ ou $b+P = P$. Portanto, A/P não possui divisores de zero e com isso é um domínio de integridade. Reciprocamente, se A/P um domínio de integridade, dados $a, b \in A$ de modo que $ab \in P$, temos $ab+P = (a+P)(b+P) = P$, donde obtemos que ou $a+P = P$ ou $b+P = P$, ou seja, $a \in P$ ou $b \in P$. Portanto, P é um ideal primo. □

Corolário 4. *Se o ideal $\langle 0 \rangle$ de um anel A é primo, então A é domínio de integridade.*

Demonstração. Se $a, b \in A$ tais que $ab = 0$, então $ab \in \langle 0 \rangle$. Mas isso nos diz que, $a \in \langle 0 \rangle$ ou $b \in \langle 0 \rangle$, isto é, $a = 0$ ou $b = 0$. Portanto, A é domínio de integridade. □

Proposição 25. *Sejam A um anel, P um ideal primo de A e $x \in A$. Se $x^n \in P$ para algum $n \in \mathbb{N}$ então $x \in P$.*

Demonstração. Suponhamos que $n \in \mathbb{N}$ é o menor natural tal que $x^n \in P$. Como P é primo, temos que $x^n = x^{n-1}x \in P$, isto é, ou $x \in P$ ou $x^{n-1} \in P$. Mas uma vez que $x^{n-1} \in P$ contradiz a minimalidade de n, segue que $x \in P$. □

Proposição 26. *Se $I_1, \cdots, I_r$ e P são ideais de A com P primo tais que $\bigcap_{i=1}^{r} I_i \subseteq P$, então $P \supseteq I_j$ para algum j. Além disso se $P = \bigcap_{i=1}^{r} I_i$, então $P = I_j$ para algum j.*

Demonstração. Suponhamos que para cada $i \in \{1, ..., n\}$ existe $x_i \in I_i$ em que $x_i \notin P$, isto é, $I_i \nsubseteq P$. Definindo $x := x_1 x_2 \cdots x_n$, onde cada um dos x_i está no seu ideal correspondente, temos que

$$x_1 x_2 \cdots x_n \in I_1 I_2 \cdots I_n \subseteq \bigcap_{i=1}^{n} I_i \Rightarrow x \in \bigcap_{i=1}^{n} I_i.$$

Como $x_i \notin P$ para cada i e P é um ideal primo, então temos que o produto $x_1 x_2 \cdots x_n \notin P$, ou seja, $x \notin P$ e portanto $\bigcap_{i=1}^{n} I_i \nsubseteq P$, o que é uma contradição.

Além disso, se $\bigcap_{i=1}^{n} I_i = P$, em particular, $\bigcap_{i=1}^{n} I_i \subseteq P$, então existe $j \in \{1, ..., n\}$ tal que $I_j \subseteq P$ tendo em vista o resultado anterior. E ainda, sendo $\bigcap_{i=1}^{n} I_i = P$ temos que P está contido em cada I_i, ou seja, $P \subseteq I_j$. Portanto $P = I_j$. □

Outros dois ideais que merecem destaque na Álgebra Comutativa são o *Nilradical* e o *Radical de Jacobson* de um anel A cujas propriedades, como veremos a seguir, são decorrentes das definições relacionadas aos ideais maximais e primos.

Proposição 27 (Nilradical)**.** *O conjunto de todos os elementos nilpotentes de um anel A é um ideal dito* ***nilradical*** *de A.*

Demonstração. Seja $\mathcal{N}$ o conjunto de todos os elementos nilpotentes de A. Então dado $x \in \mathcal{N}$,existe $n \in \mathbb{N}$ tal que $x^n = 0$, e com isso, se $\alpha \in A$, temos

$$(\alpha x)^n = \alpha^n x^n = \alpha^n 0 = 0.$$

Logo $\alpha x \in \mathcal{N}$. Além disso, dados $x, y \in \mathcal{N}$, existem $m, n \in \mathbb{N}$ tais que $x^n = 0$ e $y^m = 0$. Notemos que,

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} (-1)^i \binom{m+n}{i} x^{m+n-i} y^i.$$

Se $m+n-i \geq n$, isto é, $m \geq i$, temos $x^{m+n-i} = 0$. Caso $m < i, y^i = 0$. Em ambos os casos, cada parcela $(-1)^i \binom{m+n}{i} x^{m+n-i}(y)^i$ é igual a 0. Logo, $(x-y)^{m+n} = 0$ e disso, $x - y \in \mathcal{N}$. □

Proposição 28. *Sejam A um anel e $\mathcal{N}$ o nilradical de A. Então temos que $A/\mathcal{N}$ não possui elementos nilpotentes não nulos.*

Demonstração. Se $\overline{a} \in A/\mathcal{N}$ um elemento nilpotente, então por definição existe $n \in \mathbb{N}$ tal que $\overline{0} = (\overline{a})^n = \overline{a^n}$, isto é, $a^n \in \mathcal{N}$. Portanto, existe $m \in \mathbb{N}$ tal que $(a^n)^m = a^{nm} = 0$ e assim, temos que $a \in \mathcal{N}$. Com isso $\overline{a} = \overline{0}$.

□

Proposição 29. *O nilradical de A é a interseção de todos os ideais primos de A.*

Demonstração. Sejam $\mathcal{N}$ o nilradical de A e $S = \bigcap_{i \in \mathbb{N}} P_i$ a interseção de todos os ideais primos de A. Se $a \in \mathcal{N}$ e P é um ideal primo, uma vez que $a^k = 0$ para algum $k \in \mathbb{N}$, então existe um menor natural n tal que $a^n \in P$. Mas aplicando a Proposição 25, concluímos que $a \in P$. Uma vez que P é arbitrário, temos que $a \in S$ o que mostra que $\mathcal{N} \subseteq S$. Agora,

provaremos que $S \subseteq \mathcal{N}$, mostrando que se $a \notin \mathcal{N}$, então $a \notin S$. Seja $a \in A$ tal que $a^n \neq 0$ para todo $n \in \mathbb{N}$. Definindo

$$\mathcal{F} = \{I \subseteq A \mid a^n \notin I, \text{para todo } n \in \mathbb{N}\},$$

temos que $\mathcal{F}$ é um conjunto parcialmente ordenado pela inclusão. Note inicialmente que $\mathcal{F}$ é não vazio, pois $\langle 0 \rangle \in \mathcal{F}$. Considerando $\mathcal{C} = \{J_\alpha\}$ cadeia ascendente de ideais em $\mathcal{F}$ de modo que $J = \bigcup J_\alpha$, sendo J um ideal de A, se a^n não está contido em nenhum ideal J_α da cadeia $\mathcal{C}$, então a^n não está contido em J, o que mostra que $\mathcal{C}$ em $\mathcal{F}$ possui um limite superior. Assim, pelo Lema de Zorn, $\mathcal{F}$ possui um elemento maximal P.

Afirmação: O ideal P é primo.
Sejam $x, y \in A$ tais que $x, y \notin P$ em que $xy \in P$. Assim, P está estritamente contido nos ideais $\langle x \rangle + P$ e $\langle y \rangle + P$ e com isso, pela maximalidade de P, temos que existem $m, n \in \mathbb{N}$ tais que $a^m \in \langle x \rangle + P$ e $a^n \in \langle y \rangle + P$, isto é,

$$a^m = p' + x \text{ e } a^n = p'' + y.$$

Daí,

$$a^{m+n} = (x + p')(y + p'') = p'p'' + p'y + xp'' + xy = p + xy,$$

em que $p \in P$. Então $a^{m+n} \in \langle xy \rangle + P = P$, contradizendo o fato de P ser um elemento de $\mathcal{F}$. Com isso mostramos que P é de fato um ideal primo que não contém a e, portanto, $a \notin S$. □

Definição 40 (Radical de Jacobson)**.** *A interseção de todos os ideais maximais de A é chamado de* ***radical de Jacobson*** *e denotado por $\mathfrak{R}$.*

Proposição 30. *Vale que $x \in \mathfrak{R}$ se, e somente se, $1 - xy$ é invertível em A para todo $y \in A$.*

Demonstração. Se $1 - xy$ não é invertível, então, pelo Corolário 3, $1 - xy$ está contido num ideal maximal M. Como, por definição, $\mathfrak{R}$ é a interseção de todos os ideais maximais de A, tem-se que $\mathfrak{R} \subseteq M$. Sendo $x \in \mathfrak{R}$, temos $x \in M$. Como $x \in M$, então $1 \in M$, contradição, com o fato de que M é ideal maximal. Logo $x \notin \mathfrak{R}$.

Por outro lado, supondo $x \notin \mathfrak{R}$, então existe um ideal maximal M de A tal que $x \notin M$ e, assim, $M \subsetneq \langle x \rangle + M \subseteq A$. Mas pela definição de ideal maximal, $\langle x, M \rangle = A$, ou

seja, existe $u \in M$ de modo que $1 = u + xy$, isto é, $u = 1 - xy \in M$. Portanto $1 - xy$ não é invertível em A. □

Como todo ideal primo está em um ideal maximal, a interseção dos ideais maximais contém a interseção dos ideais primos e tal inclusão pode ser estrita, embora exemplos de tais aneis não sejam normalmente vistos em um primeiro curso de álgebra abstrata. Se todo ideal primo é a interseção dos ideais maximais que o contém, então o anel é chamado de anel de Jacobson (CONRAD, 2008, página 13).

2 Aneis Noetherianos

Os Aneis Noetherianos são de longe a classe mais importante de aneis em Álgebra Comutativa, uma vez que nos fornecem uma generalização comum dos primos da aritmética e dos tópicos de geometria (ATIYAH M.F; MACDONALF, 1969, Adaptado).

O termo Noetheriano é uma homenagem à matemática alemã *Emmy Noether* cujas contribuições matemáticas revolucionaram a Algebra Abstrata. No presente capítulo definimos e caracterizamos os Anéis Noetherianos exibindo alguns resultados e aplicações. As principais referências deste capítulo foram (MILIES, 1972) e (MARTINS; TENGAN, 2020).

Definição 41 (Anel Noetheriano)**.** *Dizemos que A é um anel* ***Noetheriano*** *se toda cadeia ascendente de ideais de A com relação a inclusão for estacionária, isto é, se*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots , \tag{2.1}$$

então existe $n_0 \in \mathbb{N}$ tal que para todo $n \geqslant n_0$ tem-se que $I_n = I_{n_0}$.

Teorema 6 (Caracterização de Aneis Noetherianos)**.** *Em um anel A as seguintes afirmações são equivalentes:*

i) A é Noetheriano;

ii) Toda família não vazia de ideais de A possui elemento maximal [1]*;*

iii) Todo ideal de A é finitamente gerado.

Demonstração. i) $\Rightarrow$ ii) Seja $\mathfrak{F}$ uma família não vazia de ideais de A tal que $\mathfrak{F}$ não possui elemento maximal. Então dado $I_0 \in \mathfrak{F}$, existe I_1 em que $I_0 \subsetneq I_1$. Como $I_1 \in \mathfrak{F}$ e $\mathfrak{F}$ não tem elemento maximal, existe $I_2 \in \mathfrak{F}$ tal que $I_1 \subsetneq I_2$. Repetindo o processo sucessivamente, construímos então

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots \tag{2.2}$$

[1] Esse elemento maximal não necessariamente é um ideal maximal, ver Definição 14.

cadeia ascendente e não estacionária. Uma[contradição, pois A é um anel Noetheriano.
ii) $\Rightarrow$ *iii)* Suponha, por absurdo, que exista I ideal de A não finitamente gerado e seja $a_0 \in I$. Então $I \neq \langle a_0 \rangle$, e portanto existe $a_1 \in I \setminus \langle a_0 \rangle$. Se $I = \langle a_0, a_1 \rangle$ teríamos que I é finitamente gerado. Logo, existe $a_2 \in I \setminus \langle a_0, a_1 \rangle$, e continuando o processo, obtemos a seguinte cadeia ascendente de ideais não estacionária

$$\langle a_0 \rangle \subsetneq \langle a_0, a_1 \rangle \subsetneq \langle a_0, a_1, a_2 \rangle \subsetneq \cdots ., \tag{2.3}$$

gerando uma contradição, pois obtemos uma família de ideais do tipo $\langle a_1, \cdots, a_i \rangle$ ordenados parcialmente pela inclusão que não possui elemento maximal.
iii) $\Rightarrow$ *i)* Dada uma cadeia ascendente de ideais de

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots, \tag{2.4}$$

considere o ideal $I = \bigcup_{n \in \mathbb{N}} I_n$. Por hipótese, I é finitamente gerado, ou seja, existem $a_1, a_2, \cdots, a_n \in A$ tais que $I = \langle a_1, a_2, ..., a_n \rangle$. Uma vez que $a_j \in I$, então existe $n_j \in \mathbb{N}$ tal que $a_j \in I_{n_j} \subseteq I$. Sendo $n_0 = max\{n_1, n_2, .., n_j\}$, então temos que $a_1, a_2, \cdots, a_{n_j} \in I_{n_0}$ e com isso

$$I = \langle a_0, a_1, ..., a_n \rangle \subseteq I_{n_0} \subseteq \bigcup_{n \in \mathbb{N}} I_n = I. \tag{2.5}$$

Desse modo, $I_{n_0} = I$ e, portanto, temos que toda cadeia ascendente de ideais de A é estacionária, isto é, A é Noetheriano. □

Exemplo 39. *Todo DIP é Noetheriano uma vez que todo ideal é finitamente gerado.*

Exemplo 40. *Se $\mathbb{K}$ é um corpo então $\mathbb{K}$ é Noetheriano. De fato, os únicos ideais de $\mathbb{K}$ são $\{0\} = \langle 0 \rangle$ e $\mathbb{K} = \langle 1 \rangle$ e ambos são finitamente gerados.*

Teorema 7 (Teorema da base de Hilbert)**.** *Se A é Noetheriano, então o anel de polinômios $A[X]$ é Noetheriano.*

Demonstração. Para mostrarmos que $A[X]$ é Noetheriano, provaremos que todo ideal de $A[X]$ é finitamente gerado. Seja I um ideal qualquer de $A[X]$. Se $I = \{0\}$ ou $I = A[X]$, então $I = \langle 0 \rangle$ ou $I = \langle 1 \rangle$, e em ambos os casos, I é finitamente gerado em $A[X]$ e, portanto, não há o que fazer. Seja então I um ideal próprio de $A[X]$ e Definamos, o subconjunto

$$J_d = \{a \in A \mid a \text{ é o coeficiente líder de algum } f(x) \in I \text{ em que } \partial(f(x)) = d\} \cup \{0\}.$$

Afirmação 1*:* O subconjunto J_d é um ideal de A. De fato, se $a, b \in J_d$, então existem $f(x),\ g(x) \in I$ com $f(x) = ax^d$ +(termos de grau menores) e $g(x) = bx^d$+(termos de grau menores) de forma que, $f(x) - g(x) = (a-b)x^d$+(termos de grau menores), de modo que $a - b \in J_d$. Além disso, se $r \in A$, dado $a \in J_d$, existe $f(x) \in A[X]$ em que $f(x) = ax^d$ +(termos de grau menores). Daí, $r \cdot f(x) = rax^d$ + (termos de grau menores), donde concluímos que $ra \in J_d$.

Afirmação 2*:* Para todo $d \in \mathbb{N}, J_d \subseteq J_{d+1}$. De fato, como $b \in J_d$, existe $g(x) \in I$ em que $g(x) = bx^d$ + (termos de grau menores). Daí, $x \cdot g(x) = bx^{d+1}$ + (termos de grau menores) $\in I$, e portanto $b \in J_{d+1}$.

Sendo A Noetheriano, existe $D \in \mathbb{N}$ tal que para todo $d \geq D$ temos,

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots \subseteq J_D = J_{D+1} = J_{D+2} = \cdots \tag{2.6}$$

cadeia ascendente estacionária de ideais finitamente gerados, ou seja, para cada $i \in \{1, \cdots, D\}$, J_i é um ideal de A. Assim, existe um conjunto B_i finito de polinômios cujos coeficientes líderes geram J_i, de modo que $\bigcup_{i=1}^{D} B_i$ é finito.

Denotando $\bigcup_{i=1}^{D} B_i = \{f_1, f_2, \cdots, f_n\}$ em que cada $f_i \in I$, temos que

$$\langle f_1, \cdots, f_n \rangle \subseteq I. \tag{2.7}$$

Por outro lado, sendo $p(x) \in I$, $p(x) \neq 0$, se $\partial(p(x)) = 0$, então existe um $k \in A$ tal que $p(x) = k$ em que $k \neq 0$. Logo, $p(x) = k \in J_0$ que é gerado pelos coeficientes líderes de $B_0 \subseteq \{f_1, \cdots, f_n\}$. Assim, existem $f_{i_1}, \cdots, f_{i_r} \in \{f_1, \cdots, f_n\}$ de grau 0 cujos coeficientes líderes geram $p(x) = k$ e desse modo, $p(x) \in \langle f_1, \cdots, f_n \rangle$.

Consideremos agora $\partial(p(x)) > 0$ de modo que exista $g(x) \in \{f_1, \cdots, f_n\}$ com $\partial(g(x)) < \partial(p(x))$ e valemos da seguinte afirmação.

Afirmação 3*:* Existe $h(x) \in \langle f_1, \cdots, f_n \rangle$ tal que $\partial(h(x)) = \partial(p(x))$ e além disso, $h(x)$ e $p(x)$ possuem o mesmo coeficiente líder.

Suponhamos $\partial(p(x)) \leq D$ e sejam $m = \partial(p(x))$ e c_p o coeficiente líder de $p(x)$. Assim, $c_p \in J_m$ em que c_p é combinação dos coeficientes líderes dos polinômios que estão em B_m, ou seja, existem $\alpha_1, \cdots, \alpha_r \in A$ tais que,

$$c_p = \alpha_1 c_{f_{i_1}} + \alpha_2 c_{f_{i_2}} + \cdots + \alpha_r c_{f_{i_r}}. \tag{2.8}$$

em que $\partial(f_{i_l}) = m$, com $l \in \{1, \cdots, r\}$. Considerando,

$$h = \alpha_1 f_{i_1} + \cdots + \alpha_r f_{i_r} \tag{2.9}$$

temos que $h \in \langle f_1, \cdots, f_n \rangle$ em que $\partial(h(x)) = m$ e o coeficiente do termo de grau m de h é dado em (2.8) com $c_p \neq 0$ e, portanto, $\partial(h(x)) = \partial(p(x))$ e $c_h = c_p$.

Suponhamos agora que $\partial(p(x)) = d > D$ temos que $J_d = J_D$. Sendo $c_p \in A$ o coeficiente líder de $p(x)$, temos $c_p \in J_d = J_D$ e, assim, existem $\beta_1, \cdots, \beta_s \in J_D$ tais que $f_{i_1}, \cdots, f_{i_s} \in B_D$, de modo que

$$c_p = \beta_1 c_{f_{i_1}} + \beta_2 c_{f_{i_2}} + \cdots + \beta_s c_{f_{i_s}}. \tag{2.10}$$

Considerando

$$h = \beta_1 x^{d-D} f_{i_1} + \cdots + \beta_s x^{d-D} f_{i_s}, \tag{2.11}$$

novamente obtemos $h \in \langle f_1, \cdots, f_n \rangle$. Sendo o coeficiente do termo de grau d de $h(x)$ dado em (2.10) com $c_p \neq 0$, temos que $h(x) \neq 0$ e $\partial(h(x)) = d = \partial(p(x))$ e, portanto, $c_h = c_p$.

Portanto, concluímos da afirmação acima que se $p(x) = h(x)$, então $p(x) \in \langle f_1, \cdots, f_n \rangle$, obtendo I finitamente gerado. Supondo $p(x) \neq h(x)$, como $\partial(p(x)) = \partial(h(x))$ e $c_h = c_p$, temos que $\partial(p(x) - h(x)) < \partial(p(x))$. Além disso, visto que $p(x), h(x) \in I \backslash \{0\}$ tem-se que $p(x) - h(x) \in \langle f_1, \cdots, f_n \rangle$ e sendo $h(x) \in \langle f_1, \cdots, f_n \rangle$ e $p(x) = (p(x) - h(x)) + h(x)$ podemos concluir que $p(x) \in \langle f_1, \cdots, f_n \rangle$. Desse modo,

$$I \subseteq \langle f_1, \cdots, f_n \rangle. \tag{2.12}$$

Assim, por (2.7) e (2.12), temos que I é finitamente gerado e, portanto, $A[X]$ é Noetheriano.

□

Corolário 5. *Se A é um anel Noetheriano, então $A[X_1, \cdots, X_n]$ é Noetheriano.*

Demonstração. Façamos a demonstração por indução sobre n. Se $n = 1$ estamos no caso do teorema acima, e portanto é válido. Suponhamos válido para $A[X_1, X_2, \cdots, X_{n-1}]$. Como $A[X_1, X_2, \cdots, X_n] = A[X_1, X_2, \cdots, X_{n-1}][X_n]$, então pelo Teorema da Base de Hilbert e pela hipótese de indução, podemos concluir que $A[X_1, \cdots, X_n]$ é Noetheriano. □

3 Decomposição Primária em Aneis Noetherianos

A decomposição primária fornece uma generalização da fatoração de um inteiro como um produto de potências de primos e a generalização correspondente a uma potência de um número primo é um ideal primário (ATIYAH M.F; MACDONALF, 1969, Adaptado).

Em razão da literatura consultada, para o presente capítulo adotaremos uma nova notação para ideais em um anel, em particular, aos ideais primários e seus respectivos resultados. As principais referências deste capítulo foram (ATIYAH M.F; MACDONALF, 1969), (ZWALD; COLEMAN, 2020) e (MARTIN, 2014).

3.1 Decomposição Primária

Começamos esta seção apresentando as definições e propriedades de um ideal radical e um ideal primário para posteriormente introduzirmos a definição de uma decomposição primária e os resultados mais pertinentes relativos a tal decomposição.

O estudo que faremos aqui servirá como base para a construção da decomposição primária de ideais em aneis Noetherianos.

Definição 42. *Se A é um anel então para cada ideal I de A, definimos o* ***radical de I*** *por*

$$\sqrt{I} = \{x \in A \mid x^n \in I \text{ para algum } n \in \mathbb{N}\}.$$

Proposição 31. *O radical de I é um ideal de A que contém I, isto é, $I \subseteq \sqrt{I}$.*

Demonstração. Note que para $I \subseteq \sqrt{I}$, pela Definição 42, basta considerarmos $n = 1$. Os demais passos da demonstração dessa proposição são análogos aos que foram feitos na Proposição 27. □

Proposição 32. *Se I e J são ideais de A, então*

$$\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}.$$

Demonstração. Uma vez que $IJ \subseteq I$ e $IJ \subseteq J$ temos que $\sqrt{IJ} \subseteq \sqrt{I}$ e $\sqrt{IJ} \subseteq \sqrt{J}$, isto é, $\sqrt{IJ} \subseteq \sqrt{I} \cap \sqrt{J}$. Por outro lado, se $x \in \sqrt{I} \cap \sqrt{J}$, então existem $n, m \in \mathbb{N}$ tais que $x^n \in I$ e $x^m \in J$. Logo, $x^n x^m = x^{n+m} \in IJ$, ou seja, $x \in \sqrt{IJ}$ e assim, $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$. Portanto, $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.

Analogamente, como $I \cap J \subseteq I$ e $I \cap J \subseteq J$, então $\sqrt{I \cap J} \subseteq \sqrt{I}$ e $\sqrt{I \cap J} \subseteq \sqrt{J}$, isto é, $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Além disso, dado $x \in \sqrt{I} \cap \sqrt{J}$, então existem $n, m \in \mathbb{N}$ tais que $x^n \in I$ e $x^m \in J$. Daí, $x^{n+m} = x^n x^m \in I \cap J$, donde vemos que, $x \in \sqrt{I \cap J}$. Portanto, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. □

Definição 43 (Ideais Radicais)**.** *Sejam A um anel e I um ideal de A. Dizemos que I é um* ***ideal radical de A*** *se $\sqrt{I} = I$.*

Proposição 33. *Se I é um ideal de A, então o radical de I é um ideal radical de A.*

Demonstração. Como $\sqrt{I}$ é um ideal de A, então $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ pela Proposição 31. Por outro lado, se $x \in \sqrt{\sqrt{I}}$, então existe $n \in \mathbb{N}$ tal que $x^n \in \sqrt{I}$. Daí, temos, por definição, que existe $m \in \mathbb{N}$ tal que $(x^n)^m = x^{nm} \in I$ e, portanto, $x \in \sqrt{I}$. □

Corolário 6. *Se I é um ideal radical de A, então $\sqrt{I^n} = I$, com $n \in \mathbb{N}$.*

Demonstração. Façamos a demonstração por indução. Para $n = 1$, temos que é válido pois $\sqrt{I} = I$ por definição. Suponhamos válido para $n > 1$, ou seja, $\sqrt{I^{n-1}} = I$. Segue da Proposição 32 que,

$$\sqrt{I^n} = \sqrt{I^{n-1} I} = \sqrt{I^{n-1}} \cap \sqrt{I} = I \cap I = I.$$

Portanto, pelo Princípio de Indução Finita, temos o resultado desejado. □

Exemplo 41. *Em um anel Noetheriano, o nilradical $\mathcal{N}$ é dado por $\mathcal{N} = \sqrt{\langle 0 \rangle}$.*

Proposição 34. *Se P é um ideal primo de A, então P é um ideal radical de A.*

Demonstração. Uma vez que P é um ideal de A, temos que $P \subseteq \sqrt{P}$. Por outro lado, se $x \in \sqrt{P}$ então existe $n \in \mathbb{N}$ tal que $x^n \in P$ logo, pela Proposição 25 temos que $x \in P$, assim, $\sqrt{P} \subseteq P$. Logo, $P = \sqrt{P}$ e, consequentemente, P é um ideal radical de A. □

Proposição 35. *Sejam $f : A \longrightarrow B$ um homomorfismo de anéis e J um ideal de B. Então*

$$\sqrt{f^{-1}(J)} = f^{-1}\left(\sqrt{J}\right).$$

Demonstração. Dado $x \in A$ tal que $x \in \sqrt{f^{-1}(J)}$, existe $n \in \mathbb{N}$ de modo que

$$x^n \in f^{-1}(J) \Leftrightarrow \ f(x^n) \in J \Leftrightarrow (f(x))^n \in J \Leftrightarrow f(x) \in \sqrt{J} \Leftrightarrow x \in f^{-1}(\sqrt{J}).$$

□

Corolário 7. *Sejam $f : A \longrightarrow B$ um homomorfismo sobrejetor de anéis e J um ideal radical de B. Então, $f^{-1}(J)$ é um ideal radical de A.*

Demonstração. Uma vez que $\sqrt{f^{-1}(J)} = f^{-1}\left(\sqrt{J}\right)$ e J é um ideal radical de B, então por definição, temos que $\sqrt{J} = J$. Assim, tomando a imagem inversa f^{-1} em ambos os lados da igualdade anterior, e utilizando a Proposição 35,

$$\sqrt{f^{-1}(J)} = f^{-1}\left(\sqrt{J}\right) = f^{-1}(J).$$

□

Definição 44 (Ideal primário)**.** *Seja A um anel e $\mathfrak{q}$ um ideal próprio de A. Dizemos que $\mathfrak{q}$ é **primário** se para quaisquer $x, y \in A$ tais que $xy \in \mathfrak{q}$ então $x \in \mathfrak{q}$ ou $y^n \in \mathfrak{q}$ para algum $n \in \mathbb{N}$.*

Exemplo 42. *Todo ideal primo é primário. De fato, se P é um ideal primo de A, então dados $x, y \in A$, se $xy \in P$, então $x \in P$ ou $y \in P$, em particular, ou $x \in P$ ou $y^n \in P$, para todo $n \in \mathbb{N}$. Portanto P é um ideal primário.*

Exemplo 43. *Os ideais $\langle 0 \rangle$ e $\langle p^n \rangle$ de $\mathbb{Z}$, com p primo, são primários.*

Teorema 8 (Caracterização de ideais primários)**.** *Seja A um anel. Então o ideal $\mathfrak{q}$ é ideal primário de A se, e somente se, o anel quociente $A/\mathfrak{q} \neq \{0 + \mathfrak{q}\}$ e todo divisor de zero em $A/\mathfrak{q}$ é nilpotente.*

Demonstração. Se $\mathfrak{q}$ é primário, então $\mathfrak{q}$ está propriamente contido em A e portanto, $A/\mathfrak{q} \neq \{0 + \mathfrak{q}\}$. Se $u + \mathfrak{q} \in A/\mathfrak{q}$ é um divisor de zero, então existe $v \notin \mathfrak{q}$ tal que

$$uv + \mathfrak{q} = \mathfrak{q} \Rightarrow uv \in \mathfrak{q}.$$

Como $v \notin \mathfrak{q}$, existe $n > 0$ tal que $u^n \in \mathfrak{q}$ e então $(u + \mathfrak{q})^n = \mathfrak{q}$.

Por outro lado, suponha que $A/\mathfrak{q} \neq \{0+\mathfrak{q}\}$ e que todo divisor de zero em $A/\mathfrak{q}$ é nilpotente. Segue que $\mathfrak{q} \subsetneq A$. Dados $x, y \in \mathfrak{q}$ tais que $xy \in \mathfrak{q}$, se $x \notin \mathfrak{q}$ então

$$(x+\mathfrak{q})(y+\mathfrak{q}) = xy + \mathfrak{q} = \mathfrak{q},$$

logo $y+\mathfrak{q}$ é um divisor de zero e existe $n > 0$ tal que

$$y^n + \mathfrak{q} = (y+\mathfrak{q})^n = \mathfrak{q} \Rightarrow y^n \in \mathfrak{q}.$$

Portanto, $\mathfrak{q}$ é um ideal primário. □

Proposição 36. *Seja $f : A \longrightarrow B$ homomorfismo sobrejetor de aneis. Se $\mathfrak{q}$ é um ideal primário de B, então $P = f^{-1}(\mathfrak{q})$ é um ideal primário de A.*

Demonstração. Se $f^{-1}(\mathfrak{q}) = A$, então $1 \in f^{-1}(\mathfrak{q})$ o que implica que $f(1) \in \mathfrak{q}$ e daí, $1 \in \mathfrak{q}$. Logo, $\mathfrak{q} = B$, uma contradição pois $\mathfrak{q} \subsetneq B$. Portanto $f^{-1}(\mathfrak{q}) \subsetneq A$. Dados, $x, y \in A$ tais que $xy \in f^{-1}(\mathfrak{q})$, então $f(xy) \in \mathfrak{q}$, o que implica que $f(x)f(y) \in \mathfrak{q}$. Sendo $\mathfrak{q}$ primário,

$$f(x) \in \mathfrak{q} \text{ ou } (f(y))^n \in \mathfrak{q} \Rightarrow f(x) \in \mathfrak{q} \text{ ou } f(y^n) \in \mathfrak{q} \Rightarrow x \in f^{-1}(\mathfrak{q}) \text{ ou } y^n \in f^{-1}(\mathfrak{q})$$

para algum $n > 0$. Portanto, $f^{-1}(\mathfrak{q})$ é primário. □

Proposição 37. *Seja $\mathfrak{q}$ um ideal primário do anel A. Então $\sqrt{\mathfrak{q}}$ é um ideal primo e, além disso, $\sqrt{\mathfrak{q}}$ é o menor ideal primo que contém $\mathfrak{q}$.*

Demonstração. Sejam $\mathfrak{q}$ um ideal primário de A e $x, y \in A$, tais que $xy \in \sqrt{\mathfrak{q}}$. Então existe $n > 0$ tal que $(xy)^n \in \mathfrak{q}$, ou seja, $x^n y^n \in \mathfrak{q}$, donde $x^n \in \mathfrak{q}$ ou $(y^n)^m \in \mathfrak{q}$ para algum $m > 0$. Mas pela definição de radical de um ideal, temos que $x \in \sqrt{\mathfrak{q}}$ ou $y \in \sqrt{\mathfrak{q}}$ e, portanto, $\sqrt{\mathfrak{q}}$ é um ideal primo.

Suponhamos agora que P é um ideal primo que contém $\mathfrak{q}$. Se $x \in \sqrt{\mathfrak{q}}$, então $x^n \in \mathfrak{q} \subset P$ para algum $n > 0$. Assim, pela Proposição 25 temos que $x \in P$ e portanto, $\sqrt{\mathfrak{q}} \subseteq P$. □

Definição 45. *Se $\mathfrak{q}$ é ideal primário em um anel A, então o ideal primo $P = \sqrt{\mathfrak{q}}$ é chamado de **primo associado** a $\mathfrak{q}$ e $\mathfrak{q}$ é dito **P-primário**.*

Segue que os elementos minimais do conjunto de primos associados ao ideal primário $\mathfrak{q}$, denotado por $Assoc(\mathfrak{q})$, são chamados de ideais primos **isolados** sempre que existir um $P_i \in Assoc(\mathfrak{q})$ em que $P_i \subseteq P$, implicar que $P_i = P$.

Proposição 38. *Se $\sqrt{\mathfrak{q}}$ é maximal, então $\mathfrak{q}$ é ideal primário. Em particular, as potências de um ideal maximal M são M-primárias.*

Demonstração. Seja $\mathfrak{q}$ ideal de A em que $M = \sqrt{\mathfrak{q}}$ com M maximal. Como $\sqrt{\mathfrak{q}}$ é a interseção de todos os ideais primos que contém $\mathfrak{q}$, se P é um ideal primo, então $M \subseteq P$.

Se M é ideal maximal, temos que $M = P$ e M é o único ideal primo de A que contém $\mathfrak{q}$. Segue-se então que $M/\mathfrak{q}$ é o único ideal primo do anel $A/\mathfrak{q}$. Como todo elemento não invertível está contido em um ideal maximal, temos que todo elemento não invertível de $A/\mathfrak{q}$ está contido em $M/\mathfrak{q}$.

Portanto, todos os elementos em M possuem potências em $\mathfrak{q}$ e todo elemento não invertível é nilpotente em $A/\mathfrak{q}$. Assim, pelo Teorema 8, como todo divisor de zero no anel $A/\mathfrak{q}$ é nilpotente, $\mathfrak{q}$ é ideal primário.

Agora, se M é maximal em A, então M é primo. Decorre da Proposição 34, que M é radical, isto é, $\sqrt{M} = M$. Se $x \in \sqrt{M^n}$ para algum $n > 0$, então existe $m > 0$ tal que $x^m \in M^n \subset M$. Daí, $x \in \sqrt{M^n} \subseteq \sqrt{M} = M$. Por outro lado, se $x \in M$, então $x^n \in M^n$, o que implica que $x \in \sqrt{M^n}$ e, assim, $M \subseteq \sqrt{M^n}$. Uma vez que $M = \sqrt{M^n}$ é maximal, M^n é primário e, além disso, M^n é um ideal M-primário. □

Exemplo 44. *Sejam $A = \mathbb{K}[x, y]$ e $\mathfrak{q} = \left\langle x, y^2 \right\rangle$. Então, $A/\mathfrak{q} \simeq \mathbb{K}[y]/\left\langle y^2 \right\rangle$ em que os divisores de zero são múltiplos de y e, portanto, nilpotentes. Aplicando o Teorema 8 segue que, $\mathfrak{q}$ é ideal primário e $P = \sqrt{\mathfrak{q}} = \langle x, y \rangle$. Desse modo*

$$P^2 \subsetneq \mathfrak{q} \subsetneq P.$$

Assim, obtemos um ideal primário que não é necessariamente uma potência de primo.

Uma interseção finita de ideais primos não é necessariamente um ideal primo. No entanto, uma interseção finita de ideais primários é primária, se impormos que todos os ideais são P-primários para um dado primo P (ZWALD; COLEMAN, 2020, página 3).

Para estabelecermos tal interseção, precisamos do resultado a seguir.

Lema 3. *Se $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$ ideais de um anel A e $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$, então*

$$\sqrt{I} = \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i}.$$

Demonstração. Se $x \in \sqrt{I}$, então existe $m > 0$ tal que $x^m \in I$, donde $x^m \in \mathfrak{q}_i$ para todo i. Assim, $x \in \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i}$ e, portanto, $\sqrt{I} \subseteq \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i}$.

Agora suponhamos que $x \in \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i}$. Então para todo i, existem $m_i > 0$ tais que $x^{m_i} \in \mathfrak{q}_i$. Sejam I ideal primário e $m = máx\{m_i\}$. Então

$$x^m \in \mathfrak{q}_i \Rightarrow x^m \in I \Rightarrow x \in \sqrt{I}.$$

Daí, $\bigcap_{i=1}^{n} \sqrt{q_i} \subseteq \sqrt{I}$ e portanto $\sqrt{I} = \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i}$. □

Teorema 9. *Sejam P um ideal primo de A e $\mathfrak{q}_1, \cdots, q_n$ ideais P-primários. Então,*

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

é P-primário.

Demonstração. Do Lema 3 e aplicando a Proposição 37, temos que

$$\sqrt{I} = \bigcap_{i=1}^{n} \sqrt{\mathfrak{q}_i} = \bigcap_{i=1}^{n} P = P.$$

Para finalizar, mostraremos que I é primário. Suponhamos que $xy \in I$, então $xy \in \mathfrak{q}_i$ para todo $i \in \{1, ..., n\}$. Além disso, se $x \notin \mathfrak{q}_j$ para algum j, então existe $m > 0$, tal que $y^m \in \mathfrak{q}_j$ donde $\mathfrak{q}_j$ é P-primário, isto é, $y \in \sqrt{\mathfrak{q}_j} = P = \sqrt{I}$. Logo existe $n > 0$ tal que $y^n \in I$ e, portanto, I é ideal primário. □

Definição 46. *Sejam I,J um ideais de A, e $a \in A$. Definimos o conjunto*

$$(I : J) = \{a \in A \mid ab \in I, \text{para todo } b \text{ em } J\}. \tag{3.1}$$

*Em particular, $(0 : J)$ é dito o **aniquilador** do ideal J e usualmente denotado por $Ann(J)$, isto é,*

$$Ann(J) = \{a \in A \mid aJ = \{0\}\}.$$

Exemplo 45. *Sejam $I \subset J$ ideais de A e $a \in A$. Então,*

$$\begin{aligned}(I : a) &= \{b \in A \mid ab \in I \subset J\} \\ &\subseteq \{b \in A \mid ab \in J\} \\ &= (J : a).\end{aligned}$$

Proposição 39. *O conjunto definido em (3.1) é um ideal do anel A, dito* ***ideal quociente****.*

Demonstração. De fato, $(I : J) \neq \emptyset$ pois $0 \in I$ e $0 \in J$, então para qualquer $b \in J$ temos que $0b = 0 \in I$. Agora, dados $x, y \in (I : J)$, temos que $xb \in I$ e $yb \in I$ para todo b em J. Assim, $xb - yb = (x - y)b \in I$ para todo $b \in J$. Além disso, para quaisquer $x \in (I : J)$e $a \in A$, temos que $ax \in (I : J)$. Daí, se $x \in (I : J)$, então para todo $b \in J, xb \in I$. Portanto, $axb \in I$ para todo $b \in J$. □

Proposição 40. *Sejam P ideal primo de A, $\mathfrak{q}$ um ideal P-primário e $a \in A$, então:*

i) Se $a \in \mathfrak{q}$, então $(\mathfrak{q} : a) = A$;

ii) Se $a \notin \mathfrak{q}$, então $(\mathfrak{q} : a)$ é P-primário;

iii) Se $a \notin P$, então $(\mathfrak{q} : a) = \mathfrak{q}$.

Demonstração. *i)* Se $a \in \mathfrak{q}$, então $1a \in \mathfrak{q}$, ou seja, $1 \in (\mathfrak{q} : a)$, o que implica que $(\mathfrak{q} : a) = A$.

ii) Se $b \in (\mathfrak{q} : a)$, então $ab \in \mathfrak{q}$ e como $\mathfrak{q}$ é primário e $a \notin \mathfrak{q}$, existe $n > 0$ tal que $b^n \in \mathfrak{q}$. Portanto, $b \in \sqrt{\mathfrak{q}} = P$ e assim nós temos

$$\mathfrak{q} \subseteq (\mathfrak{q} : a) \subseteq P.$$

Consequentemente,

$$P = \sqrt{\mathfrak{q}} \subseteq \sqrt{(\mathfrak{q} : a)} \subseteq \sqrt{P} = P,$$

e daí $\sqrt{(\mathfrak{q} : a)} = P$. Agora precisamos mostrar que $(\mathfrak{q} : a)$ é primário e desde que $a \notin \mathfrak{q}$, temos que $1 \notin (\mathfrak{q} : a)$. Daí, supondo que $xy \in (\mathfrak{q} : a)$, se $y^k \notin (\mathfrak{q} : a)$ para todo $k > 0$ então $y \notin \sqrt{(\mathfrak{q} : a)} = P$. No entanto, $xya \in \mathfrak{q}$, o que implica que $xa \in \mathfrak{q}$ ou $y^j \in \mathfrak{q}$ para algum $j > 0$, caso contrário, $y \in \sqrt{\mathfrak{q}} = P$, o que é uma contradição. Logo $xa \in \mathfrak{q}$ implica que $x \in (\mathfrak{q} : a)$. Portanto, $(\mathfrak{q} : a)$ é primário.

iii) Se $a \notin P$ e $b \in (\mathfrak{q} : a)$, então $ab \in \mathfrak{q}$. Supondo que $b \notin \mathfrak{q}$, então $a^k \in \mathfrak{q}$ para algum $k > 0$, o que implica que, $a \in \sqrt{\mathfrak{q}} = P$, contradição com o fato de $a \notin P$. Logo, $b \in \mathfrak{q}$, isto é, $(\mathfrak{q} : a) \subseteq \mathfrak{q}$.

□

Proposição 41. *Se* $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n$ *são ideais no anel* A *e* $a \in A$*, então*

$$\left(\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) : a\right) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a)$$

A demonstração dessa proposição pode ser vista em (ZWALD; COLEMAN, 2020, página 4).

Definição 47. *Sejam* A *um anel e* I *um ideal de* A*. Dizemos que* I *é um ideal* ***decomponível*** *em* A *se existirem ideais primários* $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$ *tais que o ideal* $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$*. Além disso, definimos a* ***decomposição primária*** *de um ideal* I *do anel* A *como sendo*

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i, \tag{3.2}$$

em que cada $\mathfrak{q}_i$ *é primário.*

Exemplo 46. *O ideal* $\langle 12 \rangle$ *é decomponível em* $\mathbb{Z}$ *e para verificar este fato, basta notar que* $\langle 12 \rangle = \left\langle 2^2 \right\rangle \cap \langle 3 \rangle$*. Se* $a \in \left\langle 2^2 \right\rangle \cap \langle 3 \rangle$*, então* $a \in \left\langle 2^2 \right\rangle$ *e* $a \in \langle 3 \rangle$ *logo,* $a \in \langle 12 \rangle$*. Portanto,* $\langle 12 \rangle$ *admite uma decomposição primária e tal decomposição é dada por* $\left\langle 2^2 \right\rangle \cap \langle 3 \rangle$*.*

A expressão em (3.2) é dita **minimal** se:

i) Todos os radicais $\sqrt{\mathfrak{q}_i}$ são dois a dois distintos;

ii) Tivermos que $\bigcap_{i \neq j} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$ para todo $i \in \{1, \cdots, n\}$.

Proposição 42. *Uma decomposição primária pode ser substituída por uma decomposição primária minimal.*

A demonstração dessa proposição pode ser vista em (ZWALD; COLEMAN, 2020, página 5).

Uma vez garantida a existência de uma decomposição primária minimal obtida de uma decomposição primária qualquer, enunciaremos a seguir os teoremas relativos a unicidade de tais decomposições.

Teorema 10 (Primeiro Teorema da Unicidade)**.** *Sejam* I *um ideal decomponível e* $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *uma decomposição primária minimal de* I*. Se* $P_i = \sqrt{\mathfrak{q}_i}$*, então os* $P_i's$ *são precisamente os ideais primos que ocorrem no conjunto de ideais* $\sqrt{(I : a)}$ *com* $a \in A$*, e portanto não dependem de uma decomposição particular de* I*.*

Demonstração. Sendo $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ uma decomposição primária minimal de I, para cada $a \in A$, pela Proposição 41, tem-se que

$$(I : a) = \left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) : a = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a).$$

Denote $L_a := \{j \in \{1, ..., n\} \mid a \notin \mathfrak{q}_j\}$. Então, pela Proposição 40, se $a \in \mathfrak{q}_j$, então $(\mathfrak{q}_j : a) = A$, caso contrário $a \notin \mathfrak{q}_j$, daí $(\mathfrak{q}_j : a) = \mathfrak{q}_j$. Logo,

$$\begin{cases} j \in L_a & \Rightarrow (q_j : a) = q_j. \\ j \notin L_a & \Rightarrow (q_j : a) = A. \end{cases}$$

Assim,

$$(I : a) = \bigcap_{i=1}^{n} (\mathfrak{q}_i : a) = \bigcap_{i \in L_a} (q : a) = \bigcap_{i \in L_a} \mathfrak{q}_i,$$

donde

$$\sqrt{(I : a)} = \sqrt{\bigcap_{i \in L_a} \mathfrak{q}_i} = \bigcap_{i \in L_a} \sqrt{\mathfrak{q}_i} = \bigcap_{i \in L_a} P_i.$$

Pela Proposição 26, existe $j \in L_a$ tal que $\sqrt{(I : a)} = P_j$. Por outro lado, dado $i \in \{1, ..., n\}$, como $\bigcap_{j=1}^{n} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$, então existe $a \in \bigcap_{j=1}^{n} \mathfrak{q}_j$ tal que $a \notin \mathfrak{q}_i$ com $i \neq j$. Mas uma vez que $\mathfrak{q}_i$ é P_i-primário e $a \notin \mathfrak{q}_i$, então temos que $(\mathfrak{q}_i : a)$ é P_i-primário, ou seja,

$$\sqrt{(\mathfrak{q}_i : a)} = P_i.$$

E ainda, sendo $I \subseteq \mathfrak{q}_i$, então

$$(I : a) \subseteq (\mathfrak{q}_i : a) \Rightarrow \sqrt{(I : a)} \subseteq \sqrt{(\mathfrak{q}_i : a)} = P_i \Rightarrow \sqrt{(I : a)} \subseteq P_i.$$

Para finalizar, vamos mostrar que $\mathfrak{q}_i \subseteq (I : a)$. Considerando $b \in \mathfrak{q}_i$, uma vez que $a \in \bigcap_{j=1} \mathfrak{q}_j$ para todo $i \neq j$, o produto ba está necessariamente em $\mathfrak{q}_i$ e $\mathfrak{q}_j$, ou seja,

$$ba \in \mathfrak{q}_i \bigcap \left(\bigcap_{j=1}^{n} \mathfrak{q}_j\right) = \bigcap_{l=1}^{n} \mathfrak{q}_l = I. \tag{3.3}$$

Assim, $b \in (I : a)$, logo

$$\sqrt{\mathfrak{q}_i} \subseteq \sqrt{(I : a)} \Rightarrow P_i \subseteq \sqrt{(I : a)}.$$

Portanto, $P_i = \sqrt{(I : a)}$. □

Definição 48. *Sejam A um anel e $S \subseteq A$ subconjunto não vazio. Dizemos que S é um* ***conjunto multiplicativo*** *se dados $s, t \in S$:*

i) $st \in S$;

ii) $1 \in S$.

A definição acima é apresentada, uma vez que, se faz necessária para a demonstração do Teorema a seguir. Visto que nosso trabalho tem como foco a decomposição primária em aneis Noetherianos, iremos apenas enunciá-lo e caso seja de interesse do leitor as demonstrações de tal resultado pode ser consultado em (MARTIN, 2014, páginas 84-85).

Teorema 11 (Segundo Teorema da Unicidade)**.** *Sejam I um ideal decomponível de um anel A, $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ uma decomposição primária minimal de I e $\sum = \{P_{i_1}, \cdots, P_{i_n}\}$ um conjunto isolado de ideais primos associados a I. Então $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_n}$ é independente da decomposição.*

3.2 Decomposição Primária em Aneis Noetherianos

No Capítulo 2 definimos e caracterizamos os aneis Noetherianos, agora, nesta seção faremos o estudo da decomposição primária em tais anéis.

Definição 49 (Ideal Irredutível)**.** *Sejam A anel e I,J e K ideais de A. Dizemos que I é um ideal* ***irredutível*** *se sempre que $I = J \cap K$, então ou $I = J$ ou $I = K$.*

Exemplo 47. *O ideal $\langle 0 \rangle$ é irredutível em $\mathbb{Z}$.*

Lema 4. *Em um anel Noetheriano todo ideal é uma interseção finita de ideais irredutíveis.*

Demonstração. Suponhamos que o conjunto

$$\mathcal{L} = \{I \text{ ideal de } A \text{ tal que } I \text{ não é uma interseção finita de ideais irredutíveis}\}$$

seja não vazio. Então pelo lema de Zorn, $\mathcal{L}$ possui um elemento maximal M. Note que M não é irredutível. então existem J, K ideais tais que $M = J \cap K$ em que $J \neq M \neq K$. Mas como $M \subset J$ e $M \subset K$. Pela maximalidade de M em $\mathcal{L}$, $J \notin \mathcal{L}$ e $K \notin \mathcal{L}$, ou seja, J e K são ambos uma interseção finita de ideais irredutíveis. Mas uma vez que $M = J \cap K$, temos que M também é uma interseção finita de ideais irredutíveis, contradizendo o fato de $M \in \mathcal{L}$. Portanto, $\mathcal{L}$ é vazio e o lema está provado. □

Lema 5. *Em um anel Noetheriano todo ideal irredutível é primário.*

Demonstração. Sejam A um anel Noetheriano e I um ideal irredutível de A. Considerando o anel quociente A/I e aplicando o Teorema 8, é suficiente mostrarmos que se o ideal nulo de A é irredutível então ele é primário. Dados $x, y \in A$ tais que $xy = 0$, vamos mostrar que $x = 0$ ou $y^n = 0$, para algum $n \in \mathbb{N}$. Se $x \neq 0$, considere a cadeia de ideais,

$$Ann(y) \subseteq Ann(y^2) \subseteq \cdots \subseteq Ann(y^n) \subseteq \cdots . \tag{3.4}$$

Ċomo A é Noetheriano, existe $1 \leq n \in \mathbb{N}$ tal que $Ann(y^n) = Ann(y^{n+1}) = \cdots$. A partir disso, mostraremos que se $x, y \in A$ tal que

$$Ann(y^n) = Ann(y^{n+1}) = \cdots ,$$

então $\langle x \rangle \cap \langle y^n \rangle = \langle 0 \rangle$ para algum $n > 1$.

Dado $z \in \langle x \rangle \cap \langle y^n \rangle$, então existem $v, w \in A$ tais que $z = vx = wy^n$. Daí,

$$wy^{n+1} = (wy^n)y \Rightarrow (vx)y = v(xy) = v0 = 0.$$

Portanto, wy^{n+1} implica que

$$w \in Ann(y^{n+1}) = Ann(y^n) \Rightarrow wy^n = 0,$$

isto é, $z = wy^n = 0$. Assim, $\langle x \rangle \cap \langle y^n \rangle = \langle 0 \rangle$. Como $\langle 0 \rangle$ é irredutível, temos que $\langle x \rangle = \langle 0 \rangle$ ou $\langle y^n \rangle = \langle 0 \rangle$, donde $x = 0$ ou $y^n = 0$. □

Teorema 12. *Em um anel Noetheriano, todo ideal admite uma decomposição primária.*

Demonstração. Segue imediatamente do Lema 4 e do Lema 5, pois todo ideal noetheriano é uma interseção finita de ideais irredutíveis e todo ideal irredutível é primário. □

Este resultado é frequentemente chamado de *Teorema de decomposição de Lasker-Noether*, uma vez que foi provado pela primeira vez para aneis de polinômios pelo mestre de xadrez *Emmanuel Lasker* e a prova foi posteriormente simplificada e generalizada por Emmy Noether (DUMMIT; FOOTE, 2003, página 683).

Proposição 43. *Em um anel Noetheriano, todo ideal I contém uma potência do seu radical.*

Demonstração. Sejam A um anel Noetheriano e I um ideal de A. Então $\sqrt{I}$ é finitamente gerado, ou seja, $\sqrt{I} = \langle x_1, x_2, ..., x_k \rangle$ em que $x_1, ..., x_k \in A$. Assim, por definição, existem $n_i \in \mathbb{N}$ tais que $x_i^{n_i} \in I$. Seja $N = máx\{n_i\}$. Então o ideal $(\sqrt{I})^{Nk}$ é gerado pelos elementos da forma $\left\{x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}\right\}$. em que $\sum_{j=1}^{n} i_j = Nk$. Pelo *Princípio da Casa dos Pombos*, cada um desses elementos tem pelo menos um fator $x_l^{n_l}$ com $i_l \geq N$. Então, $x_l^{i_l} \in I$ e, por isso, cada gerador de $(\sqrt{I})^{Nk}$ está em I, logo $(\sqrt{I})^{Nk} \subseteq I$. □

Corolário 8. *Em um anel Noetheriano, o nilradical $\mathcal{N}$ é nilpotente.*

Demonstração. Temos pelo Exemplo 41 que $\mathcal{N} = \sqrt{\langle 0 \rangle}$. Pela proposição anterior, $\mathcal{N}^m \subseteq \langle 0 \rangle$ para algum $m \geq 1$, donde vale a igualdade, o que prova que $\mathcal{N}$ é nilpotente. □

Proposição 44. *Sejam A um anel Noetheriano e I um ideal próprio de A. Então os ideais primos associados a I são precisamente os ideais primos que ocorrem no conjunto de ideais $(I : a)$ com $a \in A$.*

Demonstração. Pelo Primeiro Teorema de Unicidade, temos que os ideais primos associados a I são os ideais primos que ocorrem no conjunto

$$\left\{\sqrt{(I : a)} \mid a \in A\right\}.$$

Portanto, se $(I : a) = P$ é um ideal primo de A, então

$$\sqrt{(I : a)} = (I : a) = P.$$

Com isso, $(I : a)$ é um ideal primo associado a I. Reciprocamente, sejam $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ uma decomposição primária minimal de I e denotemos $I_i = \bigcap_{i \neq j} \mathfrak{q}_j \neq I$. Além disso, vimos pela demonstração do Primeiro Teorema da Unicidade que $P_i = \sqrt{(I : a)}$ para qualquer $a \in I_i$ e $a \notin \mathfrak{q}_i$, então $(I : a) \subseteq \mathfrak{q}_i$ logo $\mathfrak{q}_i$ é P_i-primário. Como A é Noetheriano, pela Proposição 43, existe $m \in \mathbb{N}$ tal que $P_i^m \subseteq \mathfrak{q}_i$ e, assim, obtemos

$$I_i P_i^m \subseteq I_i \cap P_i^m \subseteq I_i \cap \mathfrak{q}_i. \tag{3.5}$$

Seja $m \geq 1$ o menor natural tal que

$$P_i^m \subseteq \mathfrak{q}_i \text{ e } b \in I_i P_i^{m-1} \subseteq I_i \cap P_i^{m-1},$$

em que $b \notin I$. Então, $bP_i \subseteq I$ e daí temos que $(I : b) \supseteq P_i$. Além disso, como $b \in I_i$ mas $b \notin I$, segue que $b \notin \mathfrak{q}_i$. Portanto, $(I : b) \subseteq \mathfrak{q}_i$ e os ideais primos associados a I são exatamente os ideais primos da forma $(I : a)$ com $a \in A$. □

Exemplo 48. *Todo ideal do anel $\mathbb{Z}$ admite uma decomposição primária.*

Demonstração. Seja $m \in \mathbb{Z}$ tal que $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ em que cada p_i é primo e $\alpha_i \in \mathbb{N}$ com $1 \leq i \leq k$. Façamos a demonstração por indução sobre k. Notemos que se $k = 1$, então $m = p_1^{\alpha_1} \Rightarrow \langle m \rangle = \langle p_1^{\alpha_1} \rangle$ é ideal primário como visto no Exemplo 43. Suponhamos válido o resultado para k. Desse modo,

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \\ &= \left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) p_{k+1}^{\alpha_{k+1}}. \end{aligned}$$

Além disso, $mdc(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, p_{k+1}^{\alpha_{k+1}}) = 1$ e daí,

$$\begin{aligned} \langle m \rangle &= \langle p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \rangle \bigcap \left\langle p_{k+1}^{\alpha_{k+1}} \right\rangle \\ &= \langle p_1^{\alpha_1} \rangle \cap \langle p_2^{\alpha_2} \rangle \cap \cdots \cap \langle p_k^{\alpha_k} \rangle \cap \left\langle p_{k+1}^{\alpha_{k+1}} \right\rangle. \end{aligned}$$

Uma vez que cada $\langle p_i^{\alpha_i} \rangle$ é um ideal primário e $\mathbb{Z}$ é um anel Noetheriano,concluímos a demonstração. □

4 Conclusão

Nesta monografia, trouxemos a definição e caracterização dos aneis Noetherianos juntamente com sua aplicação ao *Teorema da Base de Hilbert*. Estudamos também os ideais primários e radicais para que pudéssemos, assim, posteriormente desenvolver a decomposição primária em tais aneis.

Sabemos que a decomposição de determinados objetos matemáticos se faz presente em diversas subáreas da Álgebra, sendo a principal delas, a Teoria dos Números através do Teorema Fundamental da Aritmética. Por meio deste teorema, garantimos a decomposição de qualquer número inteiro (exceto $1, -1$ ou 0) em um produto finito de números primos.

Durante o desenvolvimento do nosso trabalho, conseguimos estabelecer um paralelo entre o Teorema Fundamental da Aritmética e a decomposição primária de um ideal em um anel, em particular, em aneis Noetherianos. Devido a este fato, uma vez que os aneis dos inteiros $\mathbb{Z}$ atende todas as nossas condições para que tal decomposição exista, sua importância foi se tornando cada vez mais clara, visto que esbarramos em resultados que afirmavam que em determinados aneis, um ideal primário não é necessariamente uma potência de primo e, ainda, as potências de um ideal primo não são precisamente primárias (ver Exemplo 44).

Além disso, ao buscarmos o embasamento teórico necessário para o desenvolvimento desse trabalho, tivemos a oportunidade de revisitar conceitos vistos anteriormente em um primeiro curso de Álgebra aplicados ao objeto de estudo desta monografia.

Por fim, o que fica claro durante todo estudo referente a este trabalho, é que a Matemática pode ser cada vez mais surpreendente, pois o que num primeiro momento se tratava de um estudo sobre aneis Noetherianos e aplicações foi se tornando algo mais sólido ao decidirmos aprofundar nosso olhar entre uma dessas aplicações. Além disso, proporcionou o acesso a conteúdos que normalmente não são vistos em um primeiro curso de graduação em Matemática, possibilitando o aperfeiçoamento do senso crítico sobre o conteúdo visto através do contato constante de determinados temas. Uma possível continuidade dos estudos desenvolvidos nesse trabalho é através do estudo de tais tópicos na teoria de módulos e variedades.

Referências

ATIYAH M.F; MACDONALF, I. *Introduction To Commutative Algebra*. [S.l.]: Avalon Publishing, 1994.

BHATTACHARYA, P.; JAIN, S.; NAGPAUL, S. *Basic Abstract Algebra*. [S.l.]: Second Edition. Cambridge University Press, 1994.

CONRAD, K. *Zorn's lemma and some applications*. [S.l.], 2008. Disponível em: <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf>.

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 5ª edição reformulada. São Paulo: Atual Editora, 2003.

DUMMIT, D.; FOOTE, R. *Abstract Algebra*. [S.l.]: Third Edition. John Wiley & Sons, 2003.

HALMOS, P. *Teoria ingênua dos conjuntos: tradução de Irineu Bicudo*. São Paulo: Editora Polígono, 1970.

HEFEZ, A. *Curso de álgebra*. 5ª edição. Rio de Janeiro: IMPA, 2016. (Coleção Matemática Universitária, v. 1).

KLEINER, I. *A History of Abstract Algebra*. [S.l.]: Birkhäuser Boston, 2007.

LEQUAIN Y; GARCIA, A. *Elementos de álgebra*. 6ª edição. Rio de Janeiro: IMPA, 2005.

MARTIN, M. *Algebra Comutativa: notas de aula*. [S.l.], 2014. Disponível em: <https://www.ime.usp.br/~eugenia/algebra-comutativa/algebra_comutativa.pdf>.

MARTINS, S.; TENGAN, E. *Álgebra exemplar - um estudo da Álgebra através de exemplos*. 1ª edição. Rio de Janeiro: IMPA, 2020.

MILIES, F. *Anéis e módulos*. São Paulo: Instituto de Matemática e Estatística, Universidade de São Paulo, 1972.

ZWALD, L.; COLEMAN, R. *Primary ideals*. [S.l.], 2020. Disponível em: <https://hal.archives-ouvertes.fr/hal-03040606>.