FELIPE VIEIRA

Classes de Ideais Primos e Radicais de Anéis

Trabalho de Conclusão de Curso apresentado ao
Curso de Matemática - Habilitação Bacharelado
Departamento de Matemática
Centro de Ciências Físicas e Matemáticas
Universidade Federal de Santa Catarina

Orientador: Oscar Ricardo Janesch

Florianópolis
Novembro 2005

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no curso de Matemática - Habilitação Bacharelado e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº. 37 /CCM/05.

Profª. Carmen Suzane Comitre Gimenez
Professora responsável pela disciplina

Banca examinadora:

Oscar Ricardo Janesch
Orientador

Licio Hernanes Bezerra

Danilo Royer

Sumário

Introdução

Neste trabalho, estudamos uma classe particular de subanéis: os Ideais. Na metade do século XIX, Ernst Kummer (1810-1893) introduziu o termo “ideal”para definir uma classe de números, que ele denominou Números Ideais, e usou em uma demonstração parcial do “Último Teorema de Fermat”. Alguns anos depois, R. Dedekind (1831-1916), com base no trabalho de Kummer, definiu Ideal como sendo um subconjunto $I \subset K$, K corpo, tal que:
Se $a, b \in I$ e $m, n \in \mathbb{Z}$ então $ma + nb \in I$.

Na época de Dedekind não havia a axiomatização para definir estruturas algébricas. Para grande parte dos autores do início do século XX, corpo era uma estrutura não necessariamente comutativa, e o conceito de anel não existia.

A utilização de axiomas para definir as estruturas algébricas levou a necessidade de conhecer novas estruturas e, notadamente, as estruturas quociente. Este foi um dos impulsos para chegar à definição atual de ideal, a partir da definição de Dedekind.

Nosso principal objetivo neste trabalho é relacionar famílias de Ideais Primos com Radicais de um anel com unidade não necessariamente comutativo. Outro ponto importante do trabalho são as relações de inclusão que existem entre esses tipos de Ideais Primos e, conseqüentemente, entre os Radicais do anel.

O Capítulo 1 é um aquecimento para os outros dois Capítulos. Nele apresentaremos definições e proposições que serão úteis para o desenvolvimento dos outros capítulos. No Capítulo 2, exploraremos as Classes de Ideais Primos, apresentando suas definições, dando exemplos e estabelecendo relações entre essas classes. No Capítulo 3, último do trabalho, trabalhamos com os Radicais, mostrando as relações destes com as Classes de Ideais Primos.

Neste trabalho, todos os anéis têm unidade $1 \neq 0$. Em geral não assumimos a comutatividade para o anel. Quando for o caso, isso será explicitado. Também admitimos conhecidas as principais propriedades de subanéis.

1 Ideais

Iniciamos apresentando o conceito de ideal de um anel R como um tipo especial de subanel I de R para o qual é possível construir o anel quociente $\dfrac{R}{I}$.

Sejam R um anel e I um subanel de R. Podemos definir em R a relação

$$a \equiv b(\text{mod } I) \Leftrightarrow a - b \in I.$$

A relação acima é uma relação de equivalência em R. De fato, para $a, b, c \in R$ temos:

reflexiva:

$$a - a = 0 \in I \Rightarrow a \equiv a(\text{mod } I).$$

simétrica:

$$a \equiv b(\text{mod } I) \Rightarrow a - b \in I \Rightarrow -(a - b) = b - a \in I \Rightarrow b \equiv a(\text{mod } I).$$

transitiva:

$$\begin{aligned} a \equiv b(mod\ I)\ e\ b \equiv c(mod\ I) &\Rightarrow a - b \in I\ e\ b - c \in I \\ &\Rightarrow (a - b) + (b - c) = a - c \in I \\ &\Rightarrow a \equiv c(mod\ I). \end{aligned}$$

Vamos denotar a classe de equivalência de $a \in R$ por $\overline{a}$, isto é,

$$\overline{a} = \{b \in R; b \equiv a(\text{mod } I)\}.$$

O conjunto das classes de equivalência é denotado por

$$\frac{R}{I} = \{\overline{a}; a \in R\}.$$

Sabemos que o conjunto das classes de equivalência forma uma partição para o conjunto onde está definida a relação de equivalência. Além disso, duas classes são iguais exatamente quando seus representantes estão relacionados. Portanto,

- $R = \cup_{a \in R}\, \overline{a}$
- $\overline{a} \cap \overline{b} = \varnothing$ ou $\overline{a} = \overline{b}$

. $\overline{a} = \overline{b} \Leftrightarrow a \equiv b (\text{mod } I) \Leftrightarrow a - b \in I$.

Os conjuntos quocientes, como o que construímos acima, têm grande utilidade em matemática. Quando trabalhamos em alguma estrutura algébrica, como anel, grupo ou módulo, desejamos que o conjunto quociente preserve a estrutura algébrica. No caso da nossa construção, iniciamos com um anel R e, então, gostaríamos que $\dfrac{R}{I}$ fosse um anel, com as operações induzidas pelas operações de R.
A saber:

$$+ : \begin{array}{ll} \dfrac{R}{I} \times \dfrac{R}{I} & \rightarrow \dfrac{R}{I} \\ (\overline{x}, \overline{y}) & \mapsto \overline{x+y} \end{array} \quad ; \quad \cdot : \begin{array}{ll} \dfrac{R}{I} \times \dfrac{R}{I} & \rightarrow \dfrac{R}{I} \\ (\overline{x}, \overline{y}) & \mapsto \overline{xy} \end{array}$$

Com esta notação, temos:

Lema 1.1 *: A adição está bem definida e* $\left(\dfrac{R}{I}, +\right)$ *é grupo abeliano.*

Demonstração: Sejam $\overline{x} = \overline{a}$, $\overline{y} = \overline{b} \in \dfrac{R}{I}$. Para ver que a adição está bem definida devemos mostrar que $\overline{x+y} = \overline{a+b}$.
$\overline{x} = \overline{a} \Leftrightarrow x - a \in I$
$\overline{y} = \overline{b} \Leftrightarrow y - b \in I$
Como I é subanel vem que $x - a + y - b = (x+y) - (a+b) \in I$. Segue que $\overline{x+y} = \overline{a+b}$.
Comutatividade: $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$.
Associatividade:
$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + (\overline{y+z}) = \overline{x + (y+z)} = \overline{(x+y)+z} = (\overline{x+y}) + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}$.
Elemento Neutro: $\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$.
Elemento Simétrico: Dado $\overline{x} \in \dfrac{R}{I}$ temos que $x \in R$. Como $-x \in R$ temos a classe $\overline{-x}$. Então $\overline{x} + \overline{-x} = \overline{x + (-x)} = \overline{0}$.

■

Lema 1.2 *: Se a multiplicação está bem definida então* $\left(\dfrac{R}{I}, +, \cdot\right)$ *é anel.*

Demonstração: Em função do Lema 1.1, basta verificarmos a associatividade da multiplicação e a distributividade da multiplicação em relação à adição. Estas propriedades são mostradas de forma análoga à que fizemos no Lema 1.1 para provar a associatividade da adição.

$\blacksquare$

A conseqüência dos Lemas 1.1 e 1.2 é que:

$\dfrac{R}{I}$ **é anel se, e somente se, a multiplicação induzida está bem definida**

No entanto, não é verdade, em geral, que para todo subanel I do anel R a multiplicação esteja bem definida.

Exemplo 1.1 *: Sabemos que $\mathbb{Z}$ é subanel de $\mathbb{Q}$ e, então, temos o grupo quociente $\left(\dfrac{\mathbb{Q}}{\mathbb{Z}}, +\right)$. Afirmamos que a multiplicação induzida não está bem definida em $\dfrac{\mathbb{Q}}{\mathbb{Z}}$.*

De fato,

$\dfrac{3}{2} - \dfrac{1}{2} \in \mathbb{Z} \Rightarrow \overline{\left(\dfrac{3}{2}\right)} = \overline{\left(\dfrac{1}{2}\right)}$

$\dfrac{4}{3} - \dfrac{1}{3} \in \mathbb{Z} \Rightarrow \overline{\left(\dfrac{4}{3}\right)} = \overline{\left(\dfrac{1}{3}\right)}$

Porém $\overline{\left(\dfrac{3}{2}\right)}.\overline{\left(\dfrac{4}{3}\right)} = \overline{\left(\dfrac{12}{6}\right)} = \overline{2}$ e $\overline{\left(\dfrac{1}{2}\right)}.\overline{\left(\dfrac{1}{3}\right)} = \overline{\left(\dfrac{1}{6}\right)}$, mas $\overline{2} \neq \overline{\left(\dfrac{1}{6}\right)}$ pois $2 - \dfrac{1}{6} \notin \mathbb{Z}$.

$\blacksquare$

O Exemplo 1.1 indica que para obtermos estrutura de anel em $\dfrac{R}{I}$ com a operação induzida, devemos trabalhar com subanéis especiais.

Definição 1.1 *: Seja I um subanel do anel R. Dizemos que I é ideal à esquerda de R se $ax \in I$, para quaisquer $a \in R$ e $x \in I$.*

De outra forma: Um subconjunto I do anel R, $I \neq \varnothing$, é ideal à esquerda de R quando:

(i) $x - y \in I$, $\forall x, y \in I$

(ii) $rx \in I$, $\forall r \in R$, $\forall x \in I$.

Analogamente, definimos ideal à direita:

Definição 1.2 *: Seja I um subanel do anel R. Dizemos que I é ideal à direita de R se $xa \in I$, para quaisquer $a \in R$ e $x \in I$.*

De uma outra maneira: Um subconjunto I do anel R, $I \neq \varnothing$, é ideal à direita de R quando:

(i) $x - y \in I$, $\forall x, y \in I$

(ii) $xr \in I$, $\forall r \in R$, $\forall x \in I$.

Definição 1.3 *: Se I é ideal à direita e à esquerda, dizemos que I é ideal bilateral ou, simplesmente, ideal.*

Observação 1.1 *: Claramente, se R é um anel comutativo, essas três definições coincidem.*

Proposição 1.1 *: Seja I um subanel do anel R. São equivalentes:*

(i) $\left(\dfrac{R}{I}, +, \cdot\right)$ *é anel.*

(ii) I é ideal de R.

Demonstração: $(i) \Rightarrow (ii)$ Sejam $r \in R$ e $a \in I$. Devemos mostrar que ra, $ar \in I$.
$a = r - (r - a) \in I \Rightarrow r \equiv (r - a)(\text{mod } I) \Rightarrow \overline{r} = \overline{r - a}$.
$a = a - 0 \in I \Rightarrow a \equiv 0(\text{mod } I) \Rightarrow \overline{a} = \overline{0}$.
Como $\dfrac{R}{I}$ é anel, a multiplicação está bem definida. Então
$\overline{r}.\overline{a} = (\overline{r - a}).\overline{0} \Rightarrow \overline{ra} = \overline{0} \Rightarrow ra \in I$
$\overline{a}.\overline{r} = \overline{0}(\overline{r - a}) = \overline{ar} = \overline{0} \Rightarrow ar \in I$.
Portanto, I é ideal de R.

$(ii) \Rightarrow (i)$ De acordo com o Lema 1.2, basta provar que a multiplicação está bem definida.
Sejam $\overline{r} = \overline{s}$, $\overline{x} = \overline{y} \in \dfrac{R}{I}$. Então $r - s$, $x - y \in I$, com r, s, x, $y \in R$. Como I é ideal, temos:
$(r - s)x \in I \Rightarrow rx - sx \in I$
$s(x - y) \in I \Rightarrow sx - sy \in I$.
Segue que $rx - sx + sx - sy = rx - sy \in I$. Portanto, $\overline{r}.\overline{x} = \overline{s}.\overline{y}$ e a multiplicação está bem definida.

■

De acordo com a Proposição 1.1, os ideais de um anel são exatamente os subanéis para os quais podemos obter o anel quociente.

Observação 1.2 : *É fácil ver que, se R tem unidade 1, então $\dfrac{R}{I}$ tem unidade $\overline{1}$. Além disso, se R é comutativo, então $\dfrac{R}{I}$ é comutativo, pois $\overline{x}.\overline{y} = \overline{xy} = \overline{yx} = \overline{y}.\overline{x}$, quaisquer que sejam $\overline{x}$, $\overline{y} \in \dfrac{R}{I}$.*

A partir de agora, vamos descrever resultados sobre ideais que serão úteis nos capítulos seguintes.

Todo anel R tem pelo menos dois ideais a saber, $\{0\}$ e R. Estes ideais são chamados de **ideais triviais**.

Um ideal diferente do anel todo é chamado de **ideal próprio**.

Definição 1.4 : *Um anel R que só tem ideais triviais é chamado anel simples.*

Lema 1.3 : *Seja I um ideal à esquerda (respectivamente à direita) do anel com unidade A. Se I contém um elemento inversível de A então $I = A$.*

Demonstração: Trabalharemos com ideal à esquerda. O raciocínio para ideais à direita é o mesmo.
É claro que $I \subseteq A$.
Vamos provar a inclusão $A \subseteq I$. Seja $a \in A$. Por hipótese, existe $x \in I$ tal que $x^{-1} \in A$. Como I é ideal à esquerda de A, $x \in I$ e $ax^{-1} \in A$, temos que $a = (ax^{-1})x \in I$.
Logo, $A \subseteq I$ e, portanto, $I = A$.

$\blacksquare$

Observação 1.3 : *Se um ideal à direita ou à esquerda contém a unidade do anel, este ideal é o própio anel.*

Exemplo 1.2 : *Se K é corpo então K é um anel simples.*

Se I é um ideal não nulo de K, então existe $k \in I$, $k \neq 0$. Mas K é corpo e, daí, $k^{-1} \in K$. Como I é ideal, pelo Lema 1.3, temos que $I = K$.

$\blacksquare$

Exemplo 1.3 : *O anel $A = M_2(\mathbb{R})$ é um anel simples.*

Seja I um ideal de A e suponhamos $I \neq 0$. Assim, existe $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in I$, em que pelo menos um a_{ij} é diferente de zero, $1 \leq i, j \leq 2$. Agora, sejam $e_{rs} \in A$ $(1 \leq r, s \leq 2)$ as seguintes matrizes:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Facilmente verifica-se que $e_{rs}.\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.e_{mn}$ é uma matriz 2×2 contendo o elemento a_{sm} na posição (r, n) da matriz. Assim, como $A.I \subseteq I$ e $I.A \subseteq I$, segue que

$e_{1s}.\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.\ e_{m1} = \begin{pmatrix} a_{sm} & 0 \\ 0 & 0 \end{pmatrix} \in I$, em que $1 \leq s, m \leq 2$. Também,

$e_{2s}.\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.\ e_{m2} = \begin{pmatrix} 0 & 0 \\ 0 & a_{sm} \end{pmatrix} \in I$, em que $1 \leq s, m \leq 2$.

Daí, concluímos que, para $1 \leq s, m \leq 2$, temos:

$$\begin{pmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{pmatrix} = \begin{pmatrix} a_{sm} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{sm} \end{pmatrix} \in I.$$

Escolhamos, agora, s e m de modo que $a_{sm} \neq 0$. Assim,

$\begin{pmatrix} a_{sm}^{-1} & 0 \\ 0 & a_{sm}^{-1} \end{pmatrix} . \begin{pmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$. Mas, então, pela Observação 1.3, $I = A = M_2(\mathbb{R})$. Logo, o anel das matrizes quadradas de ordem 2 é um anel simples.

$\blacksquare$

Observação 1.4 : *O exemplo anterior é um caso particular de um teorema devido a McCoy que assegura que $M_n(K)$ é anel simples quando K é corpo.*

O exemplo abaixo mostra um procedimento para produzir ideais à direita e à esquerda.

Exemplo 1.4 *: Seja R um anel. Se $a \in R$, o conjunto $aR := \{ax; x \in R\}$ é um ideal à direita de R, chamado ideal principal gerado por a.*

É claro que aR é subanel de R. Sejam $b \in aR$ e $x \in R$. Portanto, b é da forma am, em que $m \in R$. Mas, então, $bx = amx$, ou seja, $bx \in aR$. Logo, aR é ideal à direita de R.

$\blacksquare$

De forma análoga ao que fizemos no Exemplo 1.4, temos que $Ra := \{xa; x \in R\}$ é o ideal à esquerda de R gerado por a.

Usando ideais à direita e à esquerda, podemos produzir novos ideais à direita, à esquerda e bilaterais. Para isso, introduzimos a noção de soma e produto de ideais.

Sejam I e J ideais à direita ou à esquerda do anel A. Usaremos as seguintes notações:

$$I + J = \{x + y;\ x \in I \text{ e } y \in J\}$$

$$I.J = \left\{ \sum_{i=1}^{n} x_i y_i;\ n \in \mathbb{N},\ x_i \in I \text{ e } y_i \in J \right\}.$$

Note que $I.J$ é o conjunto de todas as somas finitas de elementos de I multiplicados por elementos de J.

Proposição 1.2 *: Sejam A um anel e $I,\ J \subseteq A$. Então:*

(i) Se I e J são ideais à esquerda de A então $I + J$ é ideal à esquerda de A.

(ii) Se I e J são ideais à direita de A então $I + J$ é ideal à direita de A.

(iii) Se I é ideal à esquerda e J é ideal à esquerda ou à direita de A então $I.J$ é ideal à esquerda de A.

(iv) Se J é ideal à direita e I é ideal à esquerda ou à direita de A então $I.J$ é ideal à direita de A.

(v) Se I é ideal à esquerda e J é ideal à direita de A então $I.J$ é ideal de A.

Demonstração: (i) É claro que $I+J \neq \varnothing$ pois $I \neq \varnothing$ e $J \neq \varnothing$. Sejam $u,\ v \in I+J$. Escreva $u = a+b$, $v = c+d$ com $a,\ c \in I$ e $b,\ d \in J$. Como I e J são ideais à esquerda, temos $a-c \in I$ e $b-d \in J$. Logo,

$$u - v = (a+b) - (c+d) = (a-c) + (b-d) \in I+J.$$

Seja, agora, $\alpha \in A$. Novamente, pelo fato de I e J serem ideais à esquerda, temos $\alpha a \in I$ e $\alpha b \in J$. Logo,

$$\alpha u = \alpha(a+b) = \alpha a + \alpha b \in I+J.$$

Portanto, $I+J$ é ideal à esquerda de A.

(ii) Análoga à (i).

(iii) É claro que $I.J \neq \varnothing$, pois $I \neq \varnothing$ e $J \neq \varnothing$. Sejam $u, v \in I.J$. Então $u = \sum_{i=1}^{n} a_i b_i$, $v = \sum_{j=1}^{m} c_j d_j$ com $m,\ n \in \mathbb{N}$, $a_i,\ c_j \in I$ e $b_i,\ d_j \in J$, $i = 1, 2, \ldots, n$ e $j = 1, 2, \ldots, m$. Como I é ideal à esquerda de A, temos $(-c_j) \in I$. Logo

$$u - v = \sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} c_j d_j = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} (-c_j) d_j \in I.J.$$

Seja, agora, $\alpha \in A$. Pelo fato de I ser ideal à esquerda de A e $a_i \in I$, vem que $\alpha a_i \in I$. Logo,

$$\alpha u = \alpha \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (\alpha a_i) b_i \in I.J.$$

Portanto, $I.J$ é ideal à esquerda de A.

(iv) É análoga à (iii).

(v) Como I é ideal à esquerda, segue de (iii) que $I.J$ é ideal à esquerda. Como J é ideal à direita, segue de (iv) que $I.J$ é ideal à direita. Portanto, $I.J$ é ideal de A.

■

O exemplo abaixo mostra que, se I e J são ideais de A que não têm a mesma lateralidade, pode ocorrer que $I+J$ não seja ideal à esquerda e nem à direita de A.

Exemplo 1.5 *: Sejam* $A = M_2(\mathbb{R})$, $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ *e* $J = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$. *Facilmente verificam-se que* I *é ideal à direita, que* I *não é ideal à esquerda, que* J *é ideal à esquerda e que* J *não é ideal à direita. Verifica-se também que* $I + J = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$. *No entanto* $I + J$ *não é ideal à esquerda e nem à direita de* A.

De fato,

$$X = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in I + J,\ M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in A,$$

$$MX = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} \notin I + J$$

e

$$XM = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \notin I + J.$$

■

Definição 1.5 *: O ideal (à esquerda ou à direita)* $I + J$ *é chamado de* ***soma dos ideais*** I *e* J.

Definição 1.6 *: O ideal (à esquerda ou à direita)* $I.J$ *é chamado de* ***produto dos ideais*** I *e* J.

Exemplo 1.6 *:* $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.

É claro que $2\mathbb{Z} + 3\mathbb{Z} \subseteq \mathbb{Z}$. Por outro lado, seja $x \in \mathbb{Z}$. Como $mdc(2, 3) = 1$, aplicamos a Identidade de Bezout para garantir a existência de $r,\ s \in \mathbb{Z}$ tais que $1 = 2r + 3s$. Multiplicando-se por x, temos que $x = 2(rx) + 3(sx) \in 2\mathbb{Z} + 3\mathbb{Z}$. Portanto, $\mathbb{Z} \subseteq 2\mathbb{Z} + 3\mathbb{Z}$ e daí $\mathbb{Z} = 2\mathbb{Z} + 3\mathbb{Z}$.

■

O exemplo acima pode facilmente ser generalizado de acordo com a proposição seguinte.

Proposição 1.3 : *Sejam m, $n \in \mathbb{N}$. Então $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ em que $d =$mdc(m, n).*

Demonstração: Como $d|m$ e $d|n$, temos que $du = m$ e $dv = n$, $u, v \in \mathbb{Z}$. Isso diz que $m \in d\mathbb{Z}$ e $n \in d\mathbb{Z}$. Como $d\mathbb{Z}$ é ideal de $\mathbb{Z}$, temos que $m\mathbb{Z} \subseteq d\mathbb{Z}$ e $n\mathbb{Z} \subseteq d\mathbb{Z}$ implicam $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$.
Para ver a outra inclusão usamos a Identidade de Bezout, obtendo-se $r, s \in \mathbb{Z}$ tais que $d = mr + ns \in m\mathbb{Z} + n\mathbb{Z}$. Como $m\mathbb{Z} + n\mathbb{Z}$ é ideal temos $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$.
Portanto, $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$.

$\blacksquare$

Exemplo 1.7 : *Sabemos que $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ é ideal à esquerda de $M_2(\mathbb{R})$, e $J = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ é ideal à direita de $M_2(\mathbb{R})$. De acordo com a Proposição 1.2 (v), $I.J$ é ideal de $M_2(\mathbb{R})$. Vamos verificar que $I.J = M_2(\mathbb{R})$.*

Note que

$$x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \, x_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in I$$

e

$$y_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \, y_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in J.$$

Então

$$\begin{aligned} x_1y_1 + x_2y_2 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I.J\,. \end{aligned}$$

Como $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é a unidade de $M_2(\mathbb{R})$ que está em $I.J$, aplicamos a Observação 1.3 para concluir que $I.J = M_2(\mathbb{R})$.

■

Exemplo 1.8 *:* $RaR = \left\{ \sum_{i=1}^{n} r_i a s_i;\ n \in \mathbb{N},\ r_i,\ s_i \in \mathbb{R} \right\}$ *é ideal do anel* R*.*

Sejam R um anel e $a \in R$. Sabemos que R é ideal à esquerda de R e aR à direita de R. De acordo com a Proposição 1.2 (v), RaR é ideal de R.

■

Exemplo 1.9 *: Seja* $\{P_i\}_{i\in\Gamma}$ *uma família de ideais à esquerda (respectivamente à direita) do anel* A*. Então* $\cap_{i\in\Gamma} P_i$ *é ideal à esquerda (respectivamente à direita) de* A*.*

Faremos apenas à esquerda pois a outra situação é análoga. Como P_i é ideal à esquerda de A, temos que $0 \in P_i$ para qualquer $i \in \Gamma$, daí $\cap_{i\in\Gamma} P_i \neq \varnothing$.
Dados $x,\ y \in \cap_{i\in\Gamma} P_i$ temos que

$$x, y \in P_i, \forall i \in \Gamma \Rightarrow x - y \in P_i, \forall i \in \Gamma \Rightarrow x - y \in \cap_{i\in\Gamma} P_i.$$

Seja agora $a \in A$. Então

$$x \in P_i, \forall i \in \Gamma \Rightarrow ax \in P_i, \forall i \in \Gamma \Rightarrow ax \in \cap_{i\in\Gamma} P_i.$$

Portanto, $\cap_{i\in\Gamma} P_i$ é ideal à esquerda do anel A.

■

Observação 1.5 *: Segue do Exemplo 1.9 que a intersecção de ideais de um anel* R *é um ideal deste anel.*

Proposição 1.4 *: Seja* $\{P_i\}_{i\in\Gamma}$ *uma família de ideais à direita (respectivamente à esquerda) do anel* R*. Se* $P_i \subseteq P_j$ *ou* $P_j \subseteq P_i$ *para quaisquer* $i,\ j \in \Gamma$*, então* $\cup_{i\in\Gamma}\ P_i$ *é ideal à direita (respectivamente à esquerda) de* R*.*

Demonstração: Faremos apenas à direita, a outra situação é análoga.
Sejam $x, y \in \cup_{i\in\Gamma}\ P_i$ e $r \in R$. Então $x \in P_{i_0}$ e $y \in P_{j_0}$, para i_0 e $j_0 \in \Gamma$. Sem perda de generalidade, suponha $P_{i_0} \subseteq P_{j_0}$. Então $x,\ y \in P_{j_0}$ e como P_{j_0} é ideal à direita temos que $x - y \in P_{j_0}$ e $xr \in P_{j_0}$ e portanto $x - y$ e $xr \in \cup_{i\in\Gamma} P_i$.

■

A hipótese dos ideais estarem encaixados é indispensável para a Proposição 1.4. Veja o próximo exemplo.

Exemplo 1.10 : *$2\mathbb{Z} \cup 3\mathbb{Z} = \{x \in \mathbb{Z};\ 2|x$ ou $3|x\}$ não é ideal de $\mathbb{Z}$.*

De fato, $2,\ 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ porém $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

$\blacksquare$

Perceba que $2\mathbb{Z} \nsubseteq 3\mathbb{Z}$ e $3\mathbb{Z} \nsubseteq 2\mathbb{Z}$.

Trataremos agora de ideais primos e maximais em anéis comutativos. A idéia é apresentar aqui os resultados básicos sobre estes tipos de ideais em anéis comutativos, e abordar o caso não comutativo no capítulo seguinte.

Definição 1.7 : *Sejam R um anel comutativo e P um ideal de R, $P \neq R$. Dizemos que P é ideal primo de R se*

$$a, b \in R \text{ e } ab \in P \Rightarrow a \in P \text{ ou } b \in P.$$

Exemplo 1.11 : *Para cada número primo p, o ideal $p\mathbb{Z}$ é ideal primo do anel comutativo $\mathbb{Z}$.*

Sejam $a, b \in \mathbb{Z}$ tais que $ab \in p\mathbb{Z}$. Então $ab = pz$, em que $z \in \mathbb{Z}$. Mas, como p é primo, a ou b devem tê-lo na sua decomposição em números primos. Portanto, $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$, e $p\mathbb{Z}$ é ideal primo de $\mathbb{Z}$.

$\blacksquare$

Definição 1.8 : *Sejam R um anel comutativo e M um ideal de R, $M \neq R$. Dizemos que M é ideal maximal de R se*

$$J \text{ ideal de } R \text{ tal que } M \subseteq J \subseteq R \text{ implica } J = M \text{ ou } J = R.$$

Exemplo 1.12 : *O ideal $2\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$.*

Seja M ideal tal que $2\mathbb{Z} \subseteq M \subseteq \mathbb{Z}$. Suponha que $M \neq 2\mathbb{Z}$. Então existe $m \in M \backslash 2\mathbb{Z}$. Claro que m é da forma $2k + 1$ com $k \in \mathbb{Z}$, pois senão $m \in 2\mathbb{Z}$. Como $2k \in 2\mathbb{Z} \subseteq M$, e $2\mathbb{Z}$ é subanel de $\mathbb{Z}$, temos que $2k + 1 - 2k = 1 \in M$ e, daí, $M = \mathbb{Z}$. Portanto, $2\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$.

■

Observação 1.6 : *Um resultado clássico da Álgebra comutativa assegura que as condições abaixo são equivalentes:*

. I *é ideal de* $\mathbb{Z}$

. I *é subanel de* $\mathbb{Z}$

. $I = n\mathbb{Z}, n \in \mathbb{N}$

Usando-se o fato de que os ideais de $\mathbb{Z}$ *são da forma* $n\mathbb{Z}$*, é fácil estender o Exemplo 1.12 para um número primo qualquer, isto é,* $p\mathbb{Z}$ *é ideal maximal de* $\mathbb{Z}$*, para todo primo* p*.*

Proposição 1.5 : *Seja* R *um anel comutativo. Se* M *é um ideal maximal de* R*, então* M *é ideal primo de* R*.*

Demonstração: Seja M um ideal maximal de R. Para provar que M é ideal primo, tomamos $a, b \in R$ tais que $ab \in M$. Vamos provar que $a \in M$ ou $b \in M$. Suponha que $a \notin M$ e forme o ideal principal aR. Sabemos que a soma de ideais é ideal e, portanto, $M + aR$ é ideal de R. Como $1 \in R$, temos que $a = 0 + a.1 \in M + aR$. Mas $a \notin M$ e, então, $M \subsetneq M + aR \subseteq R$. Como M é ideal maximal de R, concluímos que $M + aR = R$. Em particular, $1 \in R = M + aR$ e, daí, existem $m \in M$ e $x \in R$ tais que $1 = m + ax$. Multiplicando por b, resulta $b = mb + (ab)x$. Sabemos que m e $ab \in M$. Então
$m \in M \Rightarrow mb \in M$
$ab \in M \Rightarrow (ab)x \in M$
$mb \in M$ e $(ab)x \in M \Rightarrow b = mb + (ab)x \in M$.
Portanto, $b \in M$ e M é ideal primo de R.

■

O próximo exemplo mostra que não vale a recíproca da Proposição 1.5, isto é, existem ideais primos que não são ideais maximais.

Exemplo 1.13 : *No anel* $\mathbb{Z}$ *o ideal* $\{0\}$ *é primo mas não é maximal.*

É claro que $\{0\}$ não é ideal maximal de $\mathbb{Z}$, pois $2\mathbb{Z}$ é ideal de $\mathbb{Z}$ e $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. Para ver que $\{0\}$ é ideal primo de $\mathbb{Z}$, tomamos $a, b \in \mathbb{Z}$ tais que $ab \in \{0\}$. Assim,

$ab = 0$ e, como $\mathbb{Z}$ é dominio, concluímos que $a = 0$ ou $b = 0$, isto é, $a \in \{0\}$ ou $b \in \{0\}$.
Portanto, $\{0\}$ é ideal primo de $\mathbb{Z}$.

$\blacksquare$

Enunciaremos agora várias definições que estão relacionadas com o Lema de Zorn.

Definição 1.9 *: Se existe uma relação de ordem no conjunto não vazio S, dizemos que S é parcialmente ordenado.*

Definição 1.10 *: Seja $\leq$ uma relação de ordem no conjunto $S \neq \varnothing$. Se, para quaisquer $x, y \in S$, vale*

$$x \leq y \text{ ou } y \leq x$$

então S é totalmente ordenado.

Definição 1.11 *: Sejam $S \neq \varnothing$ um conjunto parcialmente ordenado pela relação $\leq$ e $X \subseteq S$. Dizemos que $s \in S$ é cota superior para X quando*

$$x \leq s \text{ para todo } x \in X.$$

Definição 1.12 *: Seja S um conjunto parcialmente ordenado pela relação $\leq$. Dizemos que $s \in S$ é elemento maximal de S quando*

$$x \in S \text{ e } s \leq x \Rightarrow s = x.$$

Lema 1.4 *(Lema de Zorn) Seja S um conjunto não-vazio e parcialmente ordenado. Se todo subconjunto totalmente ordenado de S tem cota superior em S, então S tem elemento maximal.*

Demonstração: ([6], pg 105-110).

$\blacksquare$

Neste trabalho, o Lema de Zorn será importante para garantir a existência de ideais maximais em um anel R.

Teorema 1.1 *: Seja R um anel comutativo. Então existe um ideal maximal em R.*

Demonstração: Seja S o conjunto dos ideais próprios de R, isto é, ideais I tais que $I \neq R$. Então S é conjunto não-vazio, pois o ideal zero pertence a S. É claro que S é parcialmente ordenado pela relação de inclusão. Além disso, se T é um subconjunto totalmente ordenado e não-vazio de S, pela Proposição 1.4 a união de todos os ideais de T, que chamaremos de U, é um ideal. Agora, se $U = R$, então $1 \in U$ e algum $I \in T$ é tal que $1 \in I$, que implica $I = R$. Isto é um absurdo, pois S é um conjunto de ideais próprios. Logo $U \in S$ e é cota superior de T em S. Então, pelo Lema de Zorn, existe um elemento maximal M em S.
Vamos provar que M é ideal maximal de R.
De fato, como $M \in S$, temos que M é ideal próprio de R. Seja J ideal de R tal que $M \subseteq J \subsetneqq R$. Como $J \neq R$, temos que $J \in S$ e, pela maximalidade de M em S, temos que $M = J$. Portanto, M é ideal maximal de R.

$\blacksquare$

Observação 1.7 *: No Teorema 1.1 exigimos a comutatividade do anel R apenas pelo fato de termos definido ideais maximais só no caso de anéis comutativos. Note que na demonstração, a comutatividade do anel R não foi usada. Veremos no próximo capítulo que em anéis não comutativos existem os conceitos de ideal à direita maximal e ideal à esquerda maximal. Neste caso, uma demonstração totalmente análoga à feita para o Teorema 1.1 garante que um anel sempre possui ideal à direita (respectivamente à esquerda) maximal.*

Proposição 1.6 *: Para todo ideal próprio H do anel comutativo R existe um ideal maximal M tal que $H \subseteq M$. Em particular, todo anel possui ideais maximais.*

Demonstração: Considere a família Υ de todos os ideais I tais que $H \subseteq I \subsetneq R$. Obviamente, Υ é não vazio, pois $H \in \Upsilon$, e Υ é parcialmente ordenado por inclusão. Além disso, se T é subconjunto totalmente ordenado e não vazio de Υ, a união de todos os ideais de T, que chamaremos de U, é ideal e está contido em Υ. Então T tem U como cota superior. Pelo Lema de Zorn, existe M elemento maximal em Υ. Afirmamos que M é ideal maximal de R. De fato, como $M \in \Upsilon$, temos que M é ideal próprio de R. Seja J ideal de R tal que $M \subseteq J \subsetneq R$. Pela maximalidade de M em S, $M = J$. Portanto, M é ideal maximal de R e $H \subseteq M$.

$\blacksquare$

Vamos agora relacionar os anéis quocientes com os ideais primos e os ideais maximais.

Proposição 1.7 : *Sejam R um anel comutativo com unidade e I um ideal de R. Então I é ideal primo se, e somente se $\dfrac{R}{I}$ é domínio.*

Demonstração: ($\Rightarrow$) Como R é comutativo e tem unidade, segue que $\dfrac{R}{I}$ é anel comutativo com unidade. Agora, sejam $\overline{x}, \overline{y} \in \dfrac{R}{I}$ tais que $\overline{xy} = \overline{0}$ ou seja, $xy \in I$. Então, como I é primo, $x \in I$ ou $y \in I$. Portanto, $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$.

($\Leftarrow$) Sejam $x, y \in R$ tais que $xy \in I$. Como $\overline{xy} = \overline{0}$ em $\dfrac{R}{I}$, temos que $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Logo, $x \in I$ *ou* $y \in I$. Portanto, I é ideal primo.

■

Proposição 1.8 : *I é ideal maximal de um anel comutativo R com unidade se, e somente se, $\dfrac{R}{I}$ é corpo.*

Demonstração: ($\Rightarrow$) Como R é anel com unidade e comutativo, $\dfrac{R}{I}$ será anel com unidade e comutativo. Resta mostrar que todo elemento não nulo de $\dfrac{R}{I}$ tem inverso. Seja $\overline{a} \in \dfrac{R}{I}, \overline{a} \neq \overline{0}$. Então, $a \notin I$. Tomemos o ideal aR. Temos que $I \subsetneq I + aR \subseteq R$ e, como I é maximal, $I + aR = R$. Portanto, existe $r \in R$ e $i \in I$ tais que $1 = i + ar$, ou seja, $\overline{1} = \overline{i} + \overline{ar} = \overline{a}.\overline{r}$. Logo, $\overline{a}$ é inversível.

($\Leftarrow$) Seja J um ideal de R tal que $I \subseteq J \subseteq R$. Suponha $I \neq J$. Então existe $a \in J \backslash I$. Segue que $\overline{a} \neq \overline{0}$ e, como $\dfrac{R}{I}$ é corpo, existe $\overline{b} \in \dfrac{R}{I}$ tal que $\overline{a}.\overline{b} = \overline{1}$. Isso leva a $ab - 1 \in I$. Então existe $i \in I \subseteq J$ tal que $1 = ab + i$. Como $ab \in J$, temos que $1 \in J$ e, daí, $J = R$. Portanto, I é ideal maximal de R.

■

Nosso próximo passo será relacionar ideais com núcleo de homomorfismos, para então provar o Primeiro e o Segundo Teoremas do Homomorfismo.

Lembre que um homomorfismo entre os anéis R e A é uma função $f : R \to A$ tal que:

. $f(x+y) = f(x) + f(y), \forall x, y \in R$

. $f(xy) = f(x)f(y), \forall x, y \in R$.

O núcleo (ou Kernel) do homomorfismo $f : R \to A$ é o conjunto

$$\mathrm{Ker} f = \{x \in R; f(x) = 0\}.$$

As propriedades básicas de um homomorfismo $f : R \to A$ estão listadas abaixo.

. $f(0) = 0$

. $f(-x) = -f(x), \forall x \in R$

. $f(x-y) = f(x) - f(y), \forall x, y \in R$

. Se I é subanel de R então $f(I)$ é subanel de A. Em particular, fazendo $I = R$ temos que $\mathrm{Im}(f) = f(R)$ é subanel de A.

. Se I é ideal à direita (à esquerda ou bilateral) de R então $f(I)$ é ideal à direita (à esquerda ou bilateral) de $f(R)$.

. f injetor $\Leftrightarrow \mathrm{Ker} f = \{0\}$.

. Se $g : A \to B$ é homomorfismo de anéis então $g \circ f : R \to B$ é homomorfismo de anéis.

Lema 1.5 : *O núcleo do homomorfismo $f : R \to A$ é um ideal de R.*

Demonstração: Sejam $x, y \in \mathrm{Ker} f$.

$f(x-y) = f(x) - f(y) = 0 - 0 = 0 \Rightarrow x - y \in \mathrm{Ker} f$.

$f(x.y) = f(x).f(y) = 0.0 = 0 \Rightarrow x.y \in \mathrm{Ker} f$.

Isso mostra que $\mathrm{Ker} f$ é subanel de R. Para ver que é ideal, tome $r \in R$ e então:

$f(r.x) = f(r).f(x) = f(r).0 = 0 \Rightarrow r.x \in \mathrm{Ker} f$.

$f(x.r) = f(x).f(r) = 0.f(r) = 0 \Rightarrow x.r \in \mathrm{Ker} f$.

■

Exemplo 1.14 : *Homomorfismo Projeção Canônica*

Sejam A um anel e I um ideal de A. Então

$$\begin{aligned} \pi : \quad A &\to \frac{A}{I} \\ a &\mapsto \overline{a} \end{aligned}$$

é um homomorfismo, chamado Homomorfismo Projeção Canônica. De fato, dados $a, b \in A$ temos:
$\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$
$\pi(a.b) = \overline{a.b} = \overline{a}.\overline{b} = \pi(a).\pi(b)$.

$\blacksquare$

O corolário a seguir é uma espécie de recíproca do Lema 1.5, pois assegura que todo ideal do anel R é núcleo de um homomorfismo com domínio R. Este homomorfismo é exatamente o homomorfismo projeção canônica construído no Exemplo 1.14.

Corolário 1.1 : *Todo ideal do anel A é núcleo de um homomorfismo com domínio A.*

Demonstração: Seja I ideal bilateral de A. Sabemos que $\pi : A \to \dfrac{A}{I}$; $\pi(a) = \overline{a}$ é homomorfismo. Então:
$x \in I \Leftrightarrow \overline{x} = \overline{0} \Leftrightarrow \pi(x) = \overline{0} \Leftrightarrow x \in \text{Ker}(\pi)$.
Logo, $\text{Ker}(\pi) = I$.

$\blacksquare$

Recorde que um homomorfismo bijetor de anéis é chamado isomorfismo. Para indicar que existe um isomorfismo entre os anéis A e B escrevemos $A \simeq B$. Existem várias propriedades de anel que são invariantes por isomorfismo. Listamos a seguir algumas delas. Seja $f : A \to B$ um isomorfismo de anéis.
. A é comutativo $\Leftrightarrow$ B é comutativo.
. A tem unidade $\Leftrightarrow$ B tem unidade.
. A não tem divisores de zero $\Leftrightarrow$ B não tem divisores de zero.
. $a \in A$ é inversível em $A \Leftrightarrow f(a) \in B$ é inversível em B. Além disso, na direção $(\Rightarrow)$ temos que $(f(a))^{-1} = f(a^{-1})$.
. A é domínio $\Leftrightarrow$ B é domínio.
. A é corpo $\Leftrightarrow$ B é corpo.

O próximo teorema é uma das principais ferramentas no estudo de estruturas algébricas. Esse teorema envolve as definições de homomorfismo, isomorfismo, núcleo, imagem e anel quociente, e assegura que se $f : A \to B$ é homomorfismo de anéis então

$\dfrac{A}{\mathrm{Ker}(f)} \simeq \mathrm{Im}(f)$.

Teorema 1.2 *: **Primeiro Teorema do Homomorfismo***

Se $f : A \to B$ é um homomorfismo de anéis, então existe uma única função $f^* : \dfrac{A}{Ker(f)} \to Im(f)$ tal que

(i) *f^* é isomorfismo.*

(ii) *$f = i \circ f^* \circ \pi$; onde $\pi : A \to \dfrac{A}{Ker(f)}$ (projeção canônica) e $i : Im(f) \to B$ (inclusão).*

Demonstração: Defina $f^* : \dfrac{A}{\mathrm{Ker} f} \to \mathrm{Im}(f)$ por $f^*(\overline{a}) = f(a)$.

(i) f^* **bem definida** $(\Rightarrow)$ **e injetiva** $(\Leftarrow)$**:**

$$\overline{a} = \overline{b} \Leftrightarrow a - b \in \mathrm{Ker} f \Leftrightarrow f(a-b) = 0 \Leftrightarrow f(a) - f(b) = 0$$
$$\Leftrightarrow f(a) = f(b) \Leftrightarrow f^*(\overline{a}) = f^*(\overline{b}).$$

f^* **sobrejetora:**

$u \in \mathrm{Im}(f) \Rightarrow u = f(a), a \in A$.

Logo, $f^*(\overline{a}) = f(a) = u$.

f^* **homomorfismo:**

$f^*(\overline{x} + \overline{y}) = f^*(\overline{x+y}) = f(x+y) = f(x) + f(y) = f^*(\overline{x}) + f^*(\overline{y})$

$f^*(\overline{x}.\overline{y}) = f^*(\overline{x.y}) = f(x.y) = f(x).f(y) = f^*(\overline{x}).f^*(\overline{y})$

(ii) Para todo $a \in A$,

$(i \circ f^* \circ \pi)(a) = i(f^*(\overline{a})) = i(f(a)) = f(a)$,

ou seja, $i \circ f^* \circ \pi = f$.

Unicidade: Seja $g^* : \dfrac{A}{\mathrm{Ker} f} \to \mathrm{Im}(f)$ tal que $f = i \circ g^* \circ \pi$. Para $\overline{a} \in \dfrac{A}{\mathrm{Ker}(f)}$ temos que $a \in A$ e então:

$$f^*(\overline{a}) = f(a) = i(g^*(\pi(a))) = g^*(\pi(a)) = g^*(\overline{a}).$$

Logo $f^* = g^*$.

$\blacksquare$

Exemplo 1.15 *: Sejam I e J ideais do anel A tais que $I \subseteq J$. Claro que I é ideal de J.*

Então $\dfrac{\frac{A}{I}}{\frac{J}{I}} \simeq \dfrac{A}{J}$.

Seja $\varphi : \dfrac{A}{I} \to \dfrac{A}{J}$, onde $\varphi(\overline{x}) = \overline{\overline{x}}$.

φ **está bem definida:**

$\overline{x} = \overline{y} \Rightarrow x - y \in I \subseteq J \Rightarrow \overline{\overline{x}} = \overline{\overline{y}} \Rightarrow \varphi(\overline{x}) = \varphi(\overline{y})$.

Claramente φ é homomorfismo sobrejetor. **Ker**$(\varphi) = \dfrac{J}{I}$**:**

$\overline{x} \in \text{Ker}\varphi \Leftrightarrow \overline{\overline{0}} = \varphi(\overline{x}) = \overline{\overline{x}} \Leftrightarrow x - 0 \in J \Leftrightarrow \overline{x} \in \dfrac{J}{I}$.

Então, aplicando o Primeiro Teorema do Homomorfismo, $\dfrac{\frac{A}{I}}{\frac{J}{I}} \simeq \dfrac{A}{J}$. $\blacksquare$

Exemplo 1.16 *: Se $m|n$ então* $\dfrac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{\frac{m\mathbb{Z}}{n\mathbb{Z}}} \simeq \mathbb{Z}_m$.

Pela Observação 1.6, $n\mathbb{Z}$ e $m\mathbb{Z}$ são ideais de $\mathbb{Z}$ e, como $m|n$, então $n\mathbb{Z} \subseteq m\mathbb{Z}$. Portanto, pelo Exemplo 1.15, $\dfrac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{\frac{m\mathbb{Z}}{n\mathbb{Z}}} \simeq \dfrac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m$.

$\blacksquare$

Exemplo 1.17 *: Seja $A = \mathcal{C}[0,1]$ o anel das funções contínuas de $[0,1]$ em $\mathbb{R}$ com as operações usuais de soma e multiplicação de funções. Para cada $\alpha \in [0,1]$ veremos que $I_\alpha = \{f \in A; f(\alpha) = 0\}$ é ideal de A. Na verdade, é possível provar que I_α é ideal maximal.*

Considere a função

$$\begin{aligned} \varphi : \quad A &\to \mathbb{R} \\ f &\mapsto f(\alpha). \end{aligned}$$

Claramente φ é homomorfismo de anéis. Note também que φ é sobrejetora, pois dado $r \in \mathbb{R}$ basta tomar a função constante $f(x) = r \in A$ que teremos $\varphi(f) = r$. Agora,

$$f \in \mathrm{Ker}(\varphi) \Leftrightarrow \varphi(f) = 0 \Leftrightarrow f(\alpha) = 0 \Leftrightarrow f \in I_\alpha.$$

Segue que $\mathrm{Ker}(\varphi) = I_\alpha$ e, portanto, I_α é ideal de A. Pelo Primeiro Teorema do Homomorfismo, temos

$$\frac{A}{I_\alpha} \simeq \mathbb{R}.$$

Como $\mathbb{R}$ é corpo concluímos que $\dfrac{A}{I_\alpha}$ é corpo. Logo, pela Proposição 1.8, I_α é ideal maximal de $A = \mathcal{C}[0,1]$.

■

É claro que o ideal trivial (0) do anel $\mathbb{Z}$ é primo e não é maximal. O Primeiro Teorema do Homomorfismo pode ser usado para apresentar exemplos de ideais primos não triviais que não são maximais.

Exemplo 1.18 *: Se P é ideal primo do anel A então $P[x]$ é ideal primo do anel $A[x]$ mas não é maximal.*

Seja P um ideal do anel A. Considere os anéis de polinômios $A[x]$ e $\dfrac{A}{P}[x]$. Defina

$$\begin{array}{rccl} \psi : & A[x] & \rightarrow & \dfrac{A}{P}[x] \\ & \displaystyle\sum_{i=1}^{n} a_i x^i & \mapsto & \displaystyle\sum_{i=1}^{n} \overline{a_i} x^i \end{array}$$

É fácil ver que ψ é um homomorfismo sobrejetor. Vamos calcular $\mathrm{Ker}\psi$.

$$\sum_{i=1}^{n} a_i x^i \in \mathrm{Ker}\psi \Leftrightarrow \sum_{i=1}^{n} \overline{a_i} x^i = \overline{0} \Leftrightarrow \overline{a_i} = \overline{0}, \forall i \in \{1, \ldots, n\} \Leftrightarrow \sum_{i=1}^{n} a_i x^i \in P[x].$$

Segue que $\mathrm{Ker}\ \psi = P[x]$.
Pelo Primeiro Teorema do Homomorfismo temos

$$\frac{A[x]}{P[x]} \simeq \frac{A}{P}[x].$$

Agora tome P um ideal primo de A.

$$P \text{ ideal primo} \Rightarrow \frac{A}{P} \text{ domínio} \Rightarrow \frac{A}{P}[x] \text{ domínio} \Rightarrow \frac{A[x]}{P[x]} \text{ domínio} \Rightarrow P[x] \text{ ideal primo.}$$

Concluímos que, para cada ideal primo P do anel A, obtemos um ideal primo $P[x]$ do anel $A[x]$. No entanto, $P[x]$ não é ideal maximal de $A[x]$. De fato, se $P[x]$ fosse maximal teríamos que $\frac{A[x]}{P[x]}$ é corpo. Pelo isomorfismo acima $\frac{A}{P}[x]$ seria corpo. Mas isso não é possível, pois o polinômio x não tem inverso.

$\blacksquare$

Exemplo 1.19 *: Os ideais $p\mathbb{Z}[x]$, em que p é primo, são ideais primos de $\mathbb{Z}[x]$ mas não são maximais.*

Suponha que $p\mathbb{Z}[x]$ é ideal maximal, em que p é um primo qualquer.
Então $\frac{\mathbb{Z}[x]}{p\mathbb{Z}[x]} = \mathbb{Z}_p[x]$ é corpo, o que é um absurdo.

$\blacksquare$

Seja $f : A \to B$ um homomorfismo de anéis. O Segundo Teorema do Homomorfismo relaciona ideais de $f(A)$ com ideais do anel quociente $\frac{A}{\mathrm{Ker}(f)}$. Para que a demonstração deste Teorema fique mais simples, vamos provar algumas proposições relacionadas com o Segundo Teorema do Homomorfismo.

Sabemos que, se $f : A \to B$ é um homomorfismo de anéis e I é um ideal à direita (respectivamente à esquerda ou bilateral) de A, então $f(I)$ é um ideal à direita (respectivamente à esquerda ou bilateral) de $f(A)$. Agora vamos ver como ideais se comportam em relação à imagem inversa.

Proposição 1.9 *: Sejam $f : A \to B$ um homomorfismo de anéis e J um ideal à direita (à esquerda ou bilateral) de B. Então $f^{-1}(J)$ é ideal à direita (à esquerda ou bilateral) de A.*

Demonstração: Trabalharemos com ideais à direita. Para ideais à esquerda a prova é análoga e, para ideais bilaterais, é conseqüência dos casos anteriores.
Sejam $x, y \in f^{-1}(J)$ e $a \in A$. Então $x, y \in A$ e $f(x), f(y) \in J$. Como J é ideal à direita de B e $f(a) \in B$ temos:

$f(x) - f(y) \in J \Rightarrow f(x-y) \in J \Rightarrow x - y \in f^{-1}(J)$
$f(x)f(y) \in J \Rightarrow f(xy) \in J \Rightarrow xy \in f^{-1}(J)$
$f(x)f(a) \in J \Rightarrow f(xa) \in J \Rightarrow xa \in f^{-1}(J)$
Logo, $f^{-1}(J)$ é ideal à direita de A.

∎

Os itens (a) e (b) da Proposição abaixo tratam de subanéis. Portanto, também valem para ideais à direita, à esquerda ou bilaterais.

Proposição 1.10 : *Seja $f : A \to B$ um homomorfismo de anéis.*

(a) I subanel de A e $Kerf \subseteq I \Rightarrow f^{-1}(f(I)) = I$.

(b) J subanel de $B \Rightarrow f(f^{-1}(J)) = J \cap Im(f)$.

Demonstração: (a) " $\subseteq$ " :

$$\begin{aligned} x \in f^{-1}(f(I)) &\Rightarrow f(x) \in f(I) \Rightarrow f(x) = f(u), u \in I \Rightarrow f(x) - f(u) = 0 \\ &\Rightarrow f(x-u) = 0 \Rightarrow x - u \in \text{ Ker}(f) \subseteq I \Rightarrow x - u = v \in I \\ &\Rightarrow x = u + v \in I. \text{ Logo, } f^{-1}(f(I)) \subseteq I. \end{aligned}$$

" $\supseteq$ " : $x \in I \Rightarrow f(x) \in f(I) \Rightarrow x \in f^{-1}(f(I))$. Portanto, $I \subseteq f^{-1}(f(I))$

(b) " $\subseteq$ " : $x \in f(f^{-1}(J)) \Rightarrow x = f(u), u \in f^{-1}(J)$.
$u \in f^{-1}(J) \Rightarrow f(u) \in J$.
Segue que $x = f(u) \in J$. Claro que $x \in \text{Im}(f)$ e, então, concluímos que
$f(f^{-1}(J)) \subseteq J \cap \text{ Im}(f)$.
" $\supseteq$ " :

$$\begin{aligned} x \in J \cap \text{ Im}(f) &\Rightarrow x = f(u) \in J, u \in A \Rightarrow u \in f^{-1}(J) \Rightarrow f(u) \in f(f^{-1}(J)) \\ &\Rightarrow x \in f(f^{-1}(J)). \text{ Logo } J \cap \text{ Im}(f) \subseteq f(f^{-1}(J)). \end{aligned}$$

∎

Teorema 1.3 : ***Segundo Teorema do Homomorfismo***
Seja $f : A \to B$ um homomorfismo de anéis. Então existe uma correspondência biunívoca entre ideais à direita (respectivamente à esquerda ou bilaterais) de A que contém $Ker(f)$ e ideais à direita (respectivamente à esquerda ou bilaterais) de $f(A)$. Esta correspondência preserva a inclusão.

Demonstração: Trabalharemos apenas com ideais à direita. Para ideais à esquerda a prova é análoga e, para ideais bilaterais, é conseqüência dos casos anteriores.
Sejam $\Im = \{I \subseteq A; I$ é ideal à direita de A e Ker$f \subseteq I\}$ e
$\Im^* = \{J;\ J$ é ideal à direita de $f(A)\}$.
Como $f(I)$ é ideal à direita de $f(A)$, para cada $I \in \Im$, temos que
$\varphi : \Im \to \Im^*, \varphi(I) = f(I)$, está bem definida.
Para $J \in \Im^*$, a Proposição 1.9 assegura que $f^{-1}(J)$ é ideal à direita de A. Além disso:

$$\{0\} \subseteq J \Rightarrow f^{-1}(\{0\}) \subseteq f^{-1}(J) \Rightarrow \text{Ker} f \subseteq f^{-1}(J).$$

Segue que $f^{-1}(J) \in \Im$ e então

$$\psi : \Im^* \to \Im, \psi(J) = f^{-1}(J), \text{ está bem definida.}$$

Para obter a correspondência procurada, basta provar que φ é bijetora. Faremos isso mostrando que ψ é a inversa de φ.
Seja $I \in \Im$. Usando a Proposição 1.10 (a) temos:
$\psi(\varphi(I)) = \psi(f(I)) = f^{-1}(f(I)) = I$.
Seja $J \in \Im^*$. Usando a Proposição 1.10 (b) e, lembrando que $J \subseteq \text{Im}(f) = f(A)$, temos:
$\varphi(\psi(J)) = \varphi(f^{-1}(J)) = f(f^{-1}(J)) = J \cap \text{Im}(f) = J$.
Resta provar que φ e ψ preservam inclusão.
Sejam $I_1, I_2 \in \Im$ tais que $I_1 \subseteq I_2$.
$I_1 \subseteq I_2 \Rightarrow f(I_1) \subseteq f(I_2) \Rightarrow \varphi(I_1) \subseteq \varphi(I_2)$.
Sejam $J_1, J_2 \in \Im^*$ tais que $J_1 \subseteq J_2$.
$J_1 \subseteq J_2 \Rightarrow f^{-1}(J_1) \subseteq f^{-1}(J_2) \Rightarrow \psi(J_1) \subseteq \psi(J_2)$.

■

Observação 1.8 *: Revendo o que foi feito na prova do teorema anterior, podemos notar que o Segundo Teorema do Homomorfismo pode ser aplicado para subanéis em vez de ideais. No entanto, este resultado tem poucas aplicações.*

Na maioria das vezes o Segundo Teorema do Homomorfismo é usado para descrever os ideais de um anel quociente. Para fazer isso, utilizamos o Corolário seguinte.

Corolário 1.2 : *Seja I um ideal do anel A. Então existe uma correspondência biunívoca, que preserva inclusão, entre ideais à direita (à esquerda ou bilaterais) de A que contém I e ideais à direita (à esquerda ou bilaterais) do anel quociente $\dfrac{A}{I}$.*

Demonstração: Sabemos que $\pi : A \to \dfrac{A}{I}$, onde $\pi(a) = \overline{a}$, é um homomorfismo sobrejetor com $\mathrm{Ker}\pi = I$. O resultado segue aplicando o Segundo Teorema do Homomorfismo.

$\blacksquare$

Exemplo 1.20 : *Descrever os ideais do anel $\mathbb{Z}_{12} = \dfrac{\mathbb{Z}}{12\mathbb{Z}}$.*

Pelo Corolário 1.2, basta escrever os ideais de $\mathbb{Z}$ que contém $12\mathbb{Z}$. Como $\mathbb{Z}$ é domínio principal, seus ideais são da forma $n\mathbb{Z}, n \in \mathbb{Z}$.
Então, os ideais $n\mathbb{Z}$ tais que $12\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$ são obtidos tomando para n os divisores de 12. Logo, estes ideais são $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ e $12\mathbb{Z}$.
Usando a função

$$\begin{array}{rcl} \varphi : & \{I \subseteq \mathbb{Z};\ I \text{ é ideal de } \mathbb{Z} \text{ e } 12\mathbb{Z} \subseteq I\} & \to \{J;\ J \text{ ideal de } \mathbb{Z}_{12}\} \\ & I & \mapsto \pi(I) \end{array}$$

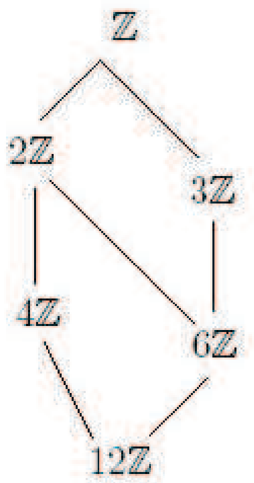
temos os ideais de $\mathbb{Z}_{12}$, em que $\pi : \mathbb{Z} \to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$, é o Homomorfismo Projeção Canônica.

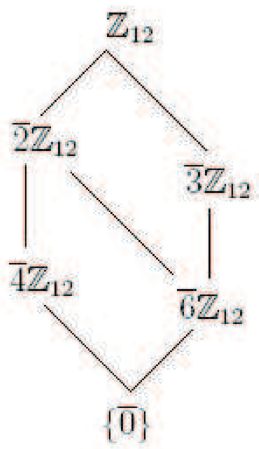
$\pi(\mathbb{Z}) = \dfrac{\mathbb{Z}}{12\mathbb{Z}}$; $\qquad \pi(2\mathbb{Z}) = \dfrac{2\mathbb{Z}}{12\mathbb{Z}} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = \overline{2}.\mathbb{Z}_{12}$

$\pi(3\mathbb{Z}) = \dfrac{3\mathbb{Z}}{12\mathbb{Z}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = \overline{3}.\mathbb{Z}_{12}$; $\qquad \pi(4\mathbb{Z}) = \dfrac{4\mathbb{Z}}{12\mathbb{Z}} = \{\overline{0}, \overline{4}, \overline{8}\} = \overline{4}.\mathbb{Z}_{12}$

$\pi(6\mathbb{Z}) = \dfrac{6\mathbb{Z}}{12\mathbb{Z}} = \{\overline{0}, \overline{6}\} = \overline{6}.\mathbb{Z}_{12}$; $\qquad \pi(12\mathbb{Z}) = \dfrac{12\mathbb{Z}}{12\mathbb{Z}} = \{\overline{0}\} = \overline{0}.\mathbb{Z}_{12}$.

O diagrama abaixo mostra as redes de ideais de $\mathbb{Z}_{12}$ e de $\mathbb{Z}$ que contêm $12\mathbb{Z}$.


$\mathbb{Z}$
$2\mathbb{Z}$
$3\mathbb{Z}$
$4\mathbb{Z}$
$6\mathbb{Z}$
$12\mathbb{Z}$


$\mathbb{Z}_{12}$
$\overline{2}\mathbb{Z}_{12}$
$\overline{3}\mathbb{Z}_{12}$
$\overline{4}\mathbb{Z}_{12}$
$\overline{6}\mathbb{Z}_{12}$
$\{\overline{0}\}$

2 Classes de Ideais Primos

Neste capítulo apresentaremos algumas classes de ideais primos e alguns exemplos. Veremos que, no caso em que R é um anel com unidade e não necessariamente comutativo, existe uma série de inclusões entre essas classes.

2.1 Ideais Primos e Ideais Completamente Primos.

Já conhecemos a definição de ideal primo em anéis comutativos (Definição 1.7). Vamos enunciá-la novamente, a fim de comparar com o caso não comutativo.

Definição 2.1 *: Seja R um anel comutativo. Dizemos que um ideal P de R é ideal primo de R quando:*

(i) $P \neq R$.

(ii) $a, b \in R$ *e* $ab \in P \Rightarrow a \in P$ *ou* $b \in P$.

Sabemos que ideais primos de anéis comutativos são úteis, entre outras aplicações, para determinar a estrutura do anel. Como exemplo, lembramos que P é ideal primo do anel comutativo R se, e somente se, $\dfrac{R}{P}$ é domínio. Em particular, R é domínio se, e somente se, (0) é ideal primo de R.

Em álgebra não comutativa, também, precisamos conhecer melhor a estrutura de um anel. Por analogia com o caso comutativo, algum tipo de ideal primo pode ser usado como ferramenta para este fim. Observando que as condições (i) e (ii) da definição anterior não dependem da comutatividade do anel, é razoável pensar em definir ideal primo em anel não comutativo da mesma forma feita para o caso comutativo. Os anos e a teoria mostraram que esta não é a boa definição, pois os ideais de um anel não comutativo que satisfazem (i) e (ii), acima, são "bastante escassos", $([3], \S 2, pg5)$. Na verdade, tais ideais, quando existem, são chamados completamente primos, como veremos adiante.

O conceito de ideal primo em anel não comutativo, que possibilita um estudo análogo ao caso comutativo, é obtido quando trocamos a condição (ii), da Definição 2.1, por outra que quantifique sobre ideais em vez de quantificar sobre elementos.

Definição 2.2 *: Seja R um anel com unidade (não necessariamente comutativo). Dizemos que um ideal P de R é ideal primo de R quando:*

(i) $P \neq R$.

(ii) Se A, B *são ideais de* R *tais que* $AB \subseteq P$ *então* $A \subseteq P$ *ou* $B \subseteq P$.

Naturalmente, no caso em que o anel R é comutativo, essas duas definições se equivalem, como veremos a seguir:

Proposição 2.1 *: Seja P um ideal próprio do anel comutativo R. São equivalentes:*

(i) $a, b \in R$ *e* $ab \in P \Rightarrow a \in P$ *ou* $b \in P$.

(ii) A, B *ideais de* R *e* $AB \subseteq P \Rightarrow A \subseteq P$ *ou* $B \subseteq P$.

Além disso, a comutatividade do anel R só é necessária para mostrar $(ii) \Rightarrow (i)$.

Demonstração: $(i) \Rightarrow (ii)$ Sejam A e B ideais de R tais que $AB \subseteq P$. Suponha que $A \nsubseteq P$ Então existe $a \in A \backslash P$. Dado $b \in B$, temos $ab \in AB \subseteq P$. Por hipótese, devemos ter $a \in P$ ou $b \in P$. Mas como $a \notin P$, resta $b \in P$. Portanto, $B \subseteq P$.

$(ii) \Rightarrow (i)$ Sejam $a, b \in R$ tais que $ab \in P$. Tome os ideais $A = aR$ e $B = bR$. Note que $AB \subseteq P$, pois se $u \in AB$ então:

$$u = \sum_{i=1}^{n} ax_i by_i, n \in \mathbb{N}, x_i y_i \in R.$$

Como R é comutativo, $ab \in P$ (ideal) e $xy \in R$ então $abxy \in P$, logo

$$u = \sum_{i=1}^{n} (ab) x_i y_i \in P.$$

Aplicando a hipótese vem que $A = aR \subseteq P$ ou $B = bR \subseteq P$, e, como R tem unidade, $a \in P$ ou $b \in P$.

■

Definição 2.3 *: Seja R um anel (não necessariamente comutativo). Dizemos que um ideal P de R é completamente primo quando:*

(i) $P \neq R$.

(ii) $a, b \in R$ *e* $ab \in P \Rightarrow a \in P$ *ou* $b \in P$.

Obviamente, se R é comutativo os ideais primos são exatamente os ideais completamente primos (Proposição 2.1).

Se R é um anel qualquer, segue da implicação $(i) \Rightarrow (ii)$ da Proposição 2.1 que todo ideal completamente primo é ideal primo. No entanto, a recíproca nem sempre é verdadeira:

Exemplo 2.1 *: Ideal primo que não é ideal completamente primo.*

Tome $R = M_2(\mathbb{R})$. Sabemos, pelo Exemplo 1.3, que esse anel é simples, ou seja, só tem os ideais triviais R e (0). Afirmamos que $P = (0)$ é ideal primo de R. De fato, sejam A e B ideais de R tais que $A.B \subseteq P = (0)$. Claro que não podemos ter $A = B = R$ pois neste caso $A.B = R.R = R \nsubseteq P$, pois R tem unidade. Logo $A = (0)$ ou $B = (0)$, isto é, $A \subseteq P$ ou $B \subseteq P$. No entanto, $P = (0)$ não é completamente primo pois

$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in R$ e $ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in P$, mas $a \notin P$ e $b \notin P$.

■

Este exemplo nos mostra que se R não é comutativo, a implicação $(ii) \Rightarrow (i)$ da Proposição 2.1 pode não valer, ou seja, a comutatividade de R é essencial para que um ideal primo seja completamente primo.

Nosso principal objetivo neste capítulo é apresentar algumas classes de ideais primos de um anel qualquer e estabelecer as relações de inclusão entre elas. Veremos ainda, além dos ideais primos e completamente primos, outros 5 tipos de ideais primos.

Vamos agora conhecer outras caracterizações dos ideais primos. Lembramos apenas que, para um anel R e $a, b \in R$, podemos formar o ideal à esquerda Rb e tomar o conjunto

$$aRb := \{axb, x \in R\}.$$

Proposição 2.2 : *Seja P um ideal do anel R tal que $P \neq R$. São equivalentes:*

(i) *P é ideal primo de R.*

(ii) *Se A, B são ideais à direita (esquerda) de R e $AB \subseteq P$ então $A \subseteq P$ ou $B \subseteq P$.*

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

(iv) *Se A, B são ideais à direita (esquerda) de R tais que $P \subseteq A, P \subseteq B$ e $AB \subseteq P$ então $A = P$ ou $B = P$.*

(v) *Se A, B são ideais bilaterais de R tais que $P \subseteq A, P \subseteq B$ e $AB \subseteq P$ então $A = P$ ou $B = P$.*

Demonstração: $(i) \Rightarrow (ii)$ Vamos fazer para ideais à direita. Sejam A, B ideais à direita de R tais que $A.B \subseteq P$. Pela Proposição 1.2 (v), $I = R.A$ e $J = R.B$ são ideais bilaterais de R e $I.J = (R.A).(R.B) \subseteq R.(A.B) \subseteq R.P \subseteq P$. Logo $I \subseteq P$ ou $J \subseteq P$. Como $1 \in R$, $\begin{cases} A \subseteq R.A = I \\ B \subseteq R.B = J \end{cases}$, e $A \subseteq P$ ou $B \subseteq P$.

$(ii) \Rightarrow (iii)$ Suponha $a, b \in R$ e $aRb \subseteq P$. Então, como P é ideal, $aRbR \subseteq P$. Mas aR e bR são ideais à direita de R daí, por hipótese, $aR \subseteq P$ ou $bR \subseteq P$. Como R tem unidade, $a \in P$ ou $b \in P$.

$(iii) \Rightarrow (iv)$ Sejam A, B ideais à direita de R tal que $P \subseteq A, P \subseteq B$ e $AB \subseteq P$. Suponhamos $A \neq P$. Como $P \subseteq A$ temos $A \nsubseteq P$. Então existe $a \in A \setminus P$. Seja $b \in B$. Dado $r \in R$, $ar \in A$ pois $a \in A$, que é ideal à direita. Agora, $arb \in AB \subseteq P$, para qualquer $r \in R$. Então, por hipótese, $a \in P$ ou $b \in P$. Como $a \notin P$, $b \in P$. Logo, $B \subseteq P$, daí, $B = P$.

$(iv) \Rightarrow (v)$ Óbvio, pois todo ideal bilateral é ideal à direita (esquerda).

$(v) \Rightarrow (i)$ Sejam A e B ideais bilaterais de R tais que $AB \subseteq P$. Note que $I = A+P$ e $J = B + P$ são ideais bilaterais de R e $P \subseteq I$ e $P \subseteq J$. Como $AB \subseteq P$ e $PB \subseteq P$ temos:
$I.J = (A + P)(B + P) \subseteq AB + P \subseteq P$, então $I = P$ ou $J = P$. Suponha $I = P$. Então $A + P = I = P$. Seja $x \in A$. Então, $x = x + 0 \in A \subseteq A + P = P$. Logo, $A \subseteq P$.

■

Se definimos ideais primos, podemos definir anéis primos:

Definição 2.4 : *Um anel R é primo quando* (0) *é ideal primo de R.*

Por definição, um ideal primo é próprio, isto é, diferente do anel. Daí, temos que o anel nulo não é anel primo, pois (0) não é ideal primo de (0).

Da definição de anel primo seguem várias relações. Uma delas é que o anel comutativo R é primo se, e somente se, R é um domínio. De fato, R é anel primo se, e somente se, (0) é ideal primo de R, e isso ocorre se, e somente se, $a, b \in R$ e $ab = 0$ implica $a = 0$ ou $b = 0$, ou seja, se, e somente se, R é um domínio. Por isso, a denominação "anel primo", no caso de anéis comutativos não é usada, pois equivale a denominação "domínio".

Como vimos no Exemplo 2.1, um anel não comutativo pode ser primo e não ser domínio, ou seja, ter divisores de zero.

Como conseqüência da Proposição 2.2, podemos obter caracterizações para anéis primos:

Proposição 2.3 : *As condições abaixo são equivalentes:*

(i) *R é anel primo*

(ii) *Se A e B são ideais à direita (esquerda) de R tais que $AB = (0)$, então $A = (0)$ ou $B = (0)$.*

(iii) *Se $a, b \in R$ e $aRb = (0)$ então $a = 0$ ou $b = 0$.*

Demonstração: $(i) \Rightarrow (ii)$ Como (0) é ideal primo, o resultado segue da Proposição 2.2 ($(i) \Rightarrow (ii)$).

$(ii) \Rightarrow (iii)$ Basta aplicar a Proposição 2.2 ($(ii) \Rightarrow (iii)$) com $P = (0)$.

$(iii) \Rightarrow (i)$ Fazendo $P = (0)$ na Proposição 2.2 ($(iii) \Rightarrow (i)$), temos que (0) é ideal primo. Logo R é anel primo.

■

Vejamos agora que um ideal primo produz um anel primo. Lembramos que a construção do anel quociente $\dfrac{R}{P}$ vista no Capítulo 1 não depende da comutatividade do anel R, mas da bilateralidade do ideal P.

Proposição 2.4 : *Seja P um ideal do anel R com $P \neq R$. São equivalentes:*

(i) P é ideal primo de R.

(ii) $\dfrac{R}{P}$ é anel primo.

Demonstração: $(i) \Rightarrow (ii)$ Inicialmente, note que $\dfrac{R}{P} \neq (\overline{0})$ pois $P \neq R$. Assim $(\overline{0}) \subsetneq \dfrac{R}{P}$ e claramente $(\overline{0})$ é ideal bilateral.
Sejam $\widehat{I}$ e $\widehat{J}$ ideais de $\dfrac{R}{P}$ tais que $\widehat{I}.\widehat{J} \subseteq (\overline{0})$. Pelo Segundo Teorema do Homomorfismo, existem ideais I e J de R tais que $P \subseteq I, P \subseteq J$ e $\dfrac{I}{P} = \widehat{I}, \dfrac{J}{P} = \widehat{J}$. Mas

$$(\overline{0}) = \widehat{I}.\widehat{J} = \frac{I}{P}.\frac{J}{P} = \frac{I.J}{P} \Rightarrow I.J \subseteq P.$$

Como P é primo por hipótese, temos $I \subseteq P$ ou $J \subseteq P$. Como as inclusões contrárias são verificadas, segue que $I = P$ ou $J = P$ e daí $\widehat{I} = \dfrac{I}{P} = \overline{0}$ ou $\widehat{J} = \dfrac{J}{P} = \overline{0}$. Logo, $(\overline{0})$ é ideal primo de $\dfrac{R}{P}$, isto é, $\dfrac{R}{P}$ é anel primo.

$(ii) \Rightarrow (i)$ Vamos usar a implicação $v) \Rightarrow i)$ da Proposição 2.2. Sejam I e J ideais de R tais que $P \subseteq I, P \subseteq J$ e $IJ \subseteq P$. Pelo Segundo Teorema do Homomorfismo, temos que $\dfrac{I}{P}$ e $\dfrac{J}{P}$ são ideais de $\dfrac{R}{P}$. Da inclusão $IJ \subseteq P$ segue que $\dfrac{I}{P}.\dfrac{J}{P} = \dfrac{IJ}{P} = (\overline{0})$. Mas por hipótese, $(\overline{0})$ é ideal primo de $\dfrac{R}{P}$, e então $\dfrac{I}{P} = (\overline{0})$ ou $\dfrac{J}{P} = (\overline{0})$. Portanto $I = P$ ou $J = P$, provando que P é ideal primo de R.

■

Observação 2.1 : *A Proposição 2.4 é a generalização da Proposição 1.7 para anéis não comutativos. De fato, vimos que um anel comutativo é primo se, e somente se, é domínio. Assim a Proposição 1.7 assegura que se R é comutativo e P é ideal de R vale:*

$$P \text{ é ideal primo} \Leftrightarrow \frac{R}{P} \text{ é anel primo.}$$

Exemplo 2.2 *Todo anel simples é anel primo.*

Se R é anel simples devemos mostrar que (0) é ideal primo de R. A prova é totalmente análoga à que fizemos no Exemplo 2.1 para verificar que (0) é ideal primo de $M_2(\mathbb{R})$.

■

O exemplo anterior fornece uma maneira para produzir exemplos de anéis primos. Para isso é necessário conhecer exemplos de anéis simples. Neste sentido há um belo resultado de classificação de anéis, devido a Wedderburn e Artin. Também temos um teorema provado por McCoy, que produz anéis simples a partir de um anel simples conhecido.

Teorema 2.1 *: **Teorema de Wedderburn - Artin***
As condições abaixo são equivalentes para um anel R.

(*i*) *R é anel artiniano e simples.*

(*ii*) *$R \simeq M_n(D)$, para um único $n \in \mathbb{N}$ e um único anel de divisão D, a menos de isomorfismo.*

Teorema 2.2 *: **Teorema de McCoy***

(*i*) *Se R é anel simples então $M_n(R)$ é anel simples.*

(*ii*) *Seja R um anel qualquer. Então J é ideal de $M_n(R)$ se, e somente se, $J = M_n(I)$ para algum ideal I de R.*

As provas dos Teoremas acima podem ser encontradas respectivamente em [8] e [7].

Note que, fazendo $n = 1$ no Teorema de Wedderburn-Artin, temos que todo anel de divisão, em particular, todo corpo, é um anel simples. Segue, por exemplo, que o anel dos quatérnios é simples e, portanto, é anel primo.

Lembre que vimos no Exemplo 1.3 que $R = M_2(\mathbb{R})$ é anel simples. Pelo Teorema de McCoy temos que $M_n(R)$, o anel de matrizes $n \times n$ cujas entradas são matrizes 2×2 reais, é anel simples e portanto é anel primo.

2.2 Ideais Fortemente Primos.

Vamos apresentar alguns conceitos e conjuntos que nos auxiliarão a definir e explorar os ideais fortemente primos.

Definição 2.5 *: Sejam R um anel e F um subconjunto de R. O anulador à direita de F em R é o conjunto $An_r(F) = \{a \in R; F.a = (0)\}$. Se $x \in R$, denotamos $An_r(\{x\})$ simplesmente por $An_r(x)$.*

Claro que de forma análoga podemos definir anulador à esquerda de F em R. No entanto, neste trabalho, utilizaremos apenas anulador à direita.

Proposição 2.5 *: Seja F um subconjunto do anel R.*

(a) $An_r(F)$ é ideal à direita de R.

(b) Se F é ideal à direita de R então $An_r(F)$ é ideal de R.

Demonstração: (a) Sejam $a, b \in An_r(F)$ e $r \in R$. Como $Fa = Fb = 0$ temos:
$u(a - b) = ua - ub = 0 - 0 = 0, \forall u \in F$ e
$u(ab) = (ua)b = 0.b = 0, \forall u \in F$.

Logo, $An_r(F)$ é subanel de R. Além disso, dado $r \in R$,

$$u(ar) = (ua)r = 0r = 0, \ \forall u \in F.$$

Então, $An_r(F)$ é ideal à direita de R.

(b) Sejam $a \in An_r(F)$ e $r \in R$. Devemos mostrar que $u(ra) = 0$ para qualquer $u \in F$, pois, daí, $ra \in An_r(F)$. Por hipótese, F é ideal à direita de R, e então $ur \in F$. Como $a \in An_r(F)$, temos que $(ur)a = u(ra) = 0$.

■

Definição 2.6 *: Um subconjunto finito F do anel R é um isolador à direita de R quando $An_r(F) = (0)$.*

Neste trabalho, usaremos apenas os isoladores à direita, então chamaremos um isolador à direita apenas de isolador. Além disso, em vez de usarmos o índice "r"(right), usaremos como índice o conjunto no qual o anulador está atuando. Por exemplo, indicaremos $An_r(F) = \{a \in R; F.a = (0)\}$ por $An_R(F)$.

Definição 2.7 : *Um anel R é fortemente primo quando todo ideal não nulo de R contém um isolador.*

Podemos definir de uma outra maneira, apenas reescrevendo a definição acima: O anel R é fortemente primo quando

$$(0) \neq I \text{ ideal de } R \Rightarrow \exists F \subseteq I, F \text{ finito, tal que } An_R(F) = (0).$$

Ou seja, R será anel fortemente primo se para cada ideal I de $R, I \neq (0)$, existe um conjunto finito $F \subseteq I$ tal que 0 é a única solução de $Fa = 0$.

Observação 2.2 : *O anel $R = (0)$ é anel fortemente primo pois não possui ideal não nulo.*

Vejamos alguns exemplos.

Exemplo 2.3 : *Todo corpo é anel fortemente primo.*

De fato, se K é corpo e $(0) \neq I$ é ideal de K, então $I = K$. Assim, $\{1\} \subseteq I$ e $An_K(1) = (0)$.

■

O Exemplo acima pode ser generalizado como segue:

Exemplo 2.4 : *Todo anel simples é anel fortemente primo.*

Se R é anel simples e $(0) \neq I$ é ideal de R, então $I = R$. Como no Exemplo anterior temos $\{1\} \subseteq I$ e $An_R(1) = (0)$.

■

Exemplo 2.5 : *Todo anel de divisão é anel fortemente primo.*

Se R é anel de divisão, então R é anel simples. Em particular o anel dos Quatérnios racionais (ou reais) é fortemente primo por ser anel simples.

■

Exemplo 2.6 : *Se n não é número primo então o anel $\mathbb{Z}_n$ não é fortemente primo.*

Como n não é primo existe $m \in \mathbb{N}$, $m \neq 1$ e $m \neq n$ tal que $m|n$. Escreva $n = mq$ com $1 < q < n$. Para ver que $\mathbb{Z}_n$ não é anel fortemente primo basta verificar que o ideal $I = \overline{m}.\mathbb{Z}_n = \{\overline{0}, \overline{m}, \overline{2m}, \ldots, \overline{(q-1)m}\}$ não contém um isolador. Observe que se $F \subseteq I$ então F só tem elementos da forma $\overline{\alpha m}$ com $\alpha \in \{0, \ldots, q-1\}$. Portanto, $An_{\mathbb{Z}_n}(F) \neq (\overline{0})$, pois $\overline{q} \in \mathbb{Z}_n$ e $\overline{\alpha m}.\overline{q} = \overline{\alpha(mq)} = \overline{\alpha n} = \overline{\alpha}\overline{0} = \overline{0}$.

■

Vamos então definir ideais fortemente primos:

Definição 2.8 : *Seja P um ideal do anel R. Dizemos que P é ideal fortemente primo de R quando:*

(i) $P \neq R$.

(ii) $\dfrac{R}{P}$ *é anel fortemente primo.*

Podemos também caracterizar os ideais fortemente primos como segue:

Proposição 2.6 : *Seja P um ideal próprio de R. As seguintes condições são equivalentes:*

(i) P é um ideal fortemente primo.

(ii) Para todo ideal $I \supset P$ existe um subconjunto finito $F \subseteq I$ tal que se $a \in R$ e $Fa \subseteq P$ então $a \in P$.

Demonstração: $(i) \Rightarrow (ii)$ Seja I ideal de R tal que $P \subset I$. Então $\dfrac{I}{P}$ é ideal de $\dfrac{R}{P}$.
Como $P \neq I$, temos que $\dfrac{I}{P} \neq \{\overline{0}\}$. Por hipótese, P é ideal fortemente primo, isto é, $\dfrac{R}{P}$ é anel fortemente primo. Segue que existe um conjunto finito $\widehat{F} \subseteq \dfrac{I}{P}$ tal que $An_{\frac{R}{P}}(\widehat{F}) = (\overline{0})$. Desde que $\widehat{F} \subseteq \dfrac{I}{P}$, podemos escrever $\widehat{F} = \dfrac{F}{P}$, $F \subseteq I$ e F finito, pois $\widehat{F}$ é finito. Devemos provar que, se $a \in R$ e $Fa \subseteq P$, então $a \in P$.

Como $Fa \subseteq P$, temos que $xa \in P$, para todo $x \in F$. Daí, $\overline{x}.\overline{a} = \overline{0}$ para todo $\overline{x} \in \widehat{F}$, isto é, $\overline{a} \in An_{\frac{R}{P}}(\widehat{F}) = (\overline{0})$. Portanto $a \in P$.

$(ii) \Rightarrow (i)$ Para provar que P é ideal fortemente primo devemos provar que $\dfrac{R}{P}$ é anel fortemente primo. Para isso, tomamos um ideal J de $\dfrac{R}{P}$, $J \neq (\overline{0})$, e devemos mostrar que existe um conjunto finito $F \subseteq J$ tal que $An_{\frac{R}{P}}(F) = (\overline{0})$. Pelo Segundo Teorema do Homomorfismo, $J = \dfrac{I}{P}$ para algum ideal I de R, e $P \subsetneqq I$ pois $J \neq (\overline{0})$. Por hipótese, existe um conjunto finito $\widehat{F} \subseteq I$ tal que $a \in R$ e $\widehat{F}a \subseteq P$ implicam $a \in P$. Tome $F = \left\{ \overline{x} \in \dfrac{R}{P};\ x \in \widehat{F} \right\}$. Note que $F \subseteq \dfrac{I}{P} = J$ e F é finito, pois $\widehat{F} \subseteq I$ é finito. Para ver que $An_{\frac{R}{P}}(F) = (\overline{0})$, tome $\overline{a} \in An_{\frac{R}{P}}(F)$. Então

$$\overline{a} \in \frac{R}{P} \text{ e } \overline{x}.\overline{a} = \overline{0}, \forall\, \overline{x} \in F \Rightarrow a \in R \text{ e } xa \in P,\ \forall x \in \widehat{F} \Rightarrow \widehat{F}a \subseteq P.$$

Logo, $a \in P$ e, portanto, $\overline{a} = \overline{0}$.

■

Observação 2.3 : *Um conjunto finito F que satisfaz a condição (ii) da Proposição 2.6 é chamado isolador módulo P.*

Corolário 2.1 : *Todo ideal primo de um anel finito é ideal fortemente primo.*

Demonstração: Seja P um ideal primo finito do anel R. Dado um ideal I de R tal que $P \subset I$ tome $F = I$. Se $a \in R$ e $Fa \subseteq P$ então $Ia \subseteq P$ e, daí, $I(aR) \subseteq P$. Como P é ideal primo, e I e aR são ideais à direita de R, temos que $I \subseteq P$ ou $aR \subseteq P$. Pela escolha de I, não temos $I \subseteq P$. Resta $aR \subseteq P$ e, como R tem unidade, vem que $a \in P$. Pela Proposição 2.6, concluímos que P é ideal fortemente primo.

■

Já vimos que todo ideal completamente primo é ideal primo. Agora, veremos como essas duas classes se relacionam com ideais fortemente primos.

Proposição 2.7 :

(a) Todo ideal fortemente primo é ideal primo.

(b) Todo ideal completamente primo é ideal fortemente primo.

Demonstração: a) Seja P um ideal fortemente primo do anel R. Para provar que P é primo tomamos ideais A e B de R tais que $P \subseteq A, P \subseteq B$ e $AB \subseteq P$. Suponha que $A \nsubseteq P$. Então $\dfrac{A}{P}$ é ideal não nulo do anel $\dfrac{R}{P}$. Por hipótese P é ideal fortemente primo e então $\frac{R}{P}$ é anel fortemente primo. Assim existe um conjunto finito $F \subseteq \frac{A}{P}$ tal que $An_{\frac{R}{P}}(F) = (\overline{0})$. A inclusão $AB \subseteq P$ assegura que $\frac{A}{P}.\frac{B}{P} = (\overline{0})$, e então temos que $F.\frac{B}{P} = (\overline{0})$. Logo $\frac{B}{P} \subseteq An_{\frac{R}{P}}(F) = (\overline{0})$ e portanto $\frac{B}{P} = (\overline{0})$. Assim $B = P$ e P é ideal primo.

b) Seja P ideal completamente primo do anel R. Para provar que P é ideal fortemente primo devemos provar que $\frac{R}{P}$ é anel fortemente primo. Para isso, tome um ideal não nulo $\widehat{I}$ de $\frac{R}{P}$. Pelo Segundo Teorema do Homomorfismo, existe um ideal I de R tal que $P \subseteq I \subseteq R$ e $\frac{I}{P} = \widehat{I}$. Como $\frac{I}{P} = \widehat{I} \neq (\overline{0})$, existe $\overline{a} \in \frac{I}{P}$ tal que $\overline{a} \neq 0$. Então, $a \in I \backslash P$. Tomemos $F = \{\overline{a}\} \subseteq \widehat{I}$. Vamos provar que $An_{\frac{R}{P}}(F) = (\overline{0})$. Dado $\overline{b} \in An_{\frac{R}{P}}(F)$, temos que $\overline{b} \in \frac{R}{P}$ e $\overline{a}\overline{b} = \overline{0}$. Assim $ab \in P$ e, como P é ideal completamente primo e $a \notin P$, vem que $b \in P$. Portanto, $\overline{b} = \overline{0}$, isto é, $An_{\frac{R}{P}}(F) = (\overline{0})$.

■

Exemplo 2.7 : *Ideal fortemente primo que não é completamente primo.*

Vimos no Exemplo 2.1 que o ideal $P = (0)$ do anel $M_2(\mathbb{R})$ não é completamente primo. Por outro lado, como $M_2(\mathbb{R})$ é anel simples, segue do Exemplo 2.4 que $M_2(\mathbb{R})$ é anel fortemente primo. Portanto, $P = (0)$ é ideal fortemente primo que não é completamente primo.

■

Na literatura sobre classes de ideais primos encontra-se a afirmação que a classe de ideais fortemente primos não coincide com a classe de ideais primos. No entanto, nenhum exemplo, ou sequer um caminho para produzir um exemplo de ideal primo que não é fortemente primo, é apresentado. Tentamos em vão produzir um exemplo. Claro que tal exemplo deve ser procurado entre os anéis não simples e não comutativos, pois os anéis simples são fortemente primos (Exemplo 2.4), e nos anéis comutativos os ideais primos são completamente primos (Proposição 2.1) e, então, são fortemente primos (Proposição 2.7 (b)). Outra restrição para obter o tal exemplo são os anéis finitos. De fato, se P é ideal primo e o anel é finito, então P é fortemente primo (Corolário 2.1). Em particular, devemos procurar em anéis infinitos. Também não tivemos sucesso na busca do exemplo desejado em anéis da forma $M_n(A)$, em que A não é anel de divisão. Não procuramos em anéis de matrizes infinitas e anéis de grupos, pois um estudo destes anéis fogem do objetivo do trabalho.

2.3 Ideais Primos não Singulares.

Definição 2.9 : *Um ideal à direita H de R é dito essencial se para todo ideal à direita $I \neq (0)$ de R temos $I \cap H \neq (0)$.*

Exemplo 2.8 : *Seja R um anel primo. Então todo ideal não nulo H é ideal essencial como ideal à direita.*

De fato, seja $I \neq (0)$ ideal à direita de R. Então, como R é anel primo e H e I são não nulos, $IH \neq (0)$. Mas, note que $IH \subseteq I \cap H$, pois se $r \in IH, r = \sum_{i=1}^{n} x_i y_i, x_i \in I$, $y_i \in H$. Ora, se $x_i \in I, I$ é ideal à direita e $y_i \in H \subseteq R$, temos que $x_i y_i \in I$, e se $y_i \in H$, H é ideal e $x_i \in I \subseteq R$ temos $x_i y_i \in H$. Logo, $r \in I \cap H$. Portanto, $(0) \neq IH \subseteq I \cap H$ e H é ideal essencial.

■

Exemplo 2.9 : *Os ideais essenciais de $\mathbb{Z}_4$ são $\mathbb{Z}_4$ e $\overline{2}.\mathbb{Z}_4 = \{\overline{0}, \overline{2}\}$.*

De fato, os únicos ideais de $\mathbb{Z}_4$ são $\{\overline{0}\}, \overline{2}\mathbb{Z}_4$ e $\mathbb{Z}_4$. Logo, todo ideal não nulo de $\mathbb{Z}_4$ tem intersecção não trivial com $\overline{2}\mathbb{Z}_4$ e com $\mathbb{Z}_4$.

■

Vimos na Proposição 2.5 (a) que $An_R(a)$ é ideal à direita de R. A definição abaixo diz que o conjunto dos elementos $a \in R$, para os quais o ideal $An_R(a)$ é essencial, formam o ideal singular.

Definição 2.10 : *O ideal singular (à direita) $Z(R)$ de R é definido como o conjunto dos elementos $a \in R$ tais que $An_R(a)$ é ideal essencial.*

Para provar que $Z(R)$ é, de fato, um ideal de R usaremos o seguinte lema.

Lema 2.1 *: Sejam I um ideal essencial de R e $x \in R$. Então $J_x = \{r \in R;\ xr \in I\}$ é ideal essencial de R.*

Demonstração: Como $0 \in J_x$, temos que $J_x \neq \varnothing$.
Sejam $r_1, r_2 \in J_x$. Então, $xr_1, xr_2 \in I$, e segue que:
$x(r_1 - r_2) = xr_1 - xr_2 \in I \Rightarrow r_1 - r_2 \in J_x$,
$x(r_1.r_2) = (xr_1)r_2 \in I \Rightarrow r_1.r_2 \in J_x$
Logo J_x é subanel de R.
Dado $\lambda \in R$, temos que $xr_1\lambda \in I$, pois $xr_1 \in I$. Então, $r_1\lambda \in J_x$, e J_x é ideal à direita de R.
Suponha que J_x não seja ideal essencial. Então existe um ideal à direita H de R tal que $H \neq (0)$ e $H \cap J_x = (0)$.
Como H é ideal à direita, é fácil ver que $H' = xH$ é ideal à direita de R.
Afirmamos que $H' \cap I = (0)$. De fato, se $u \in H' \cap I$ então $u = xh \in I$, $h \in H \subseteq R$. Pela definição do conjunto J_x, temos que $h \in J_x$. Logo, $h \in J_x \cap H = (0)$, e daí $h = 0$, o que implica em $u = xh = 0$.
Como I é ideal essencial de R e $H' \cap I = (0)$, devemos ter $H' = (0)$. Vamos ver que isso leva a uma contradição. Como $H \neq (0)$, podemos tomar $0 \neq h_1 \in H$.
Então $xh_1 \in xH = H' = (0)$, e daí $xh_1 = 0$, que implica em $h_1 \in J_x$. Portanto, $0 \neq h_1 \in J_x \cap H = (0)$. Absurdo.

■

Observação 2.4 *: Na prova do Lema 2.1, só usamos a hipótese de I ser ideal essencial de R para mostrar que J_x é ideal essencial de R. Portanto, se I é ideal à direita de R então J_x é ideal à direita de R.*

Proposição 2.8 *: $Z(R)$ é ideal de R.*

Demonstração: Inicialmente, note que $Z(R) \neq \varnothing$, pois $An_R(0) = R$, que é ideal essencial de R, e então $0 \in Z(R)$.
Sejam $a, b \in Z(R)$. Então $An_R(a)$ e $An_R(b)$ são ideais essenciais. Seja I um ideal à direita de R, $I \neq (0)$. Como $An_R(a)$ é ideal essencial, temos que $J = I \cap An_R(a)$ é ideal à direita de R e $J \neq (0)$. Como $An_R(b)$ é ideal essencial temos que $(0) \neq J \cap An_R(b)$.
Então:

$$(0) \neq J \cap An_R(b) = I \cap (An_R(a) \cap An_R(b)) \subseteq I \cap An_R(a-b).$$

Segue que $An_R(a-b)$ é ideal essencial de R e, assim, $a-b \in Z(R)$.
Da mesma forma prova-se que $(0) \neq I \cap An_R(a.b)$ e, então, $ab \in Z(R)$.
Até aqui temos provado que $Z(R)$ é subanel de R.
Para verificar que $Z(R)$ é ideal à esquerda de R, tomamos $x \in R$, e observamos que $An_R(a) \subseteq An_R(xa)$. Como $An_R(a)$ é ideal essencial, temos que para todo ideal à direita I de R, $I \neq (0)$, vale $(0) \neq I \cap An_R(a)$ e, então, $(0) \neq I \cap An_R(xa)$. Portanto, $An_R(xa)$ é ideal essencial de R e, então, $xa \in Z(R)$.
Falta verificar que $Z(R)$ é ideal à direita de R.
Com a notação estabelecida acima devemos mostrar que $I \cap An_R(ax) \neq (0)$ para todo ideal à direita I de R, $I \neq (0)$.
Como $An_R(a)$ é ideal essencial de R, segue do Lema 2.1 que
$J_x = \{r \in R;\ xr \in An_R(a)\}$ é ideal essencial de R. Note ainda que:

$$r \in J_x \Rightarrow xr \in An_R(a) \Rightarrow axr = 0 \Rightarrow r \in An_R(ax).$$

Assim $J_x \subseteq An_R(ax)$.
Desde que J_x é ideal essencial de R temos:
$(0) \neq I \cap J_x \subseteq I \cap An_R(ax) \Rightarrow An_R(ax)$ é ideal essencial de R.
Portanto $xa \in Z(R)$ e $Z(R)$ é ideal à direita de R.

$\blacksquare$

Definição 2.11 : *Um anel R é não singular (à direita) se $Z(R) = (0)$.*

Neste trabalho, não exploraremos os anéis não singulares e, sim, ideais não singulares, e para isso usaremos a seguinte definição:

Definição 2.12 : *Um ideal primo P de R é dito ideal primo não singular se $\dfrac{R}{P}$ é um anel não singular, ou seja, $Z\left(\dfrac{R}{P}\right) = 0$.*

Exemplo 2.10 : *O ideal (0) é ideal primo não singular do anel $\mathbb{Z}$.*

Como $\mathbb{Z}$ é domínio temos que (0) é ideal completamente primo e, portanto, é ideal primo.
Seja $x \in Z(\mathbb{Z})$. Então $An_{\mathbb{Z}}(x)$ é ideal essencial de $\mathbb{Z}$. Como os ideais de $\mathbb{Z}$ são da

forma $n.\mathbb{Z}$, existe $n \in \mathbb{N}$ tal que $An_{\mathbb{Z}}(x) = n.\mathbb{Z}$.
Se $n = 0$ vem que $An_{\mathbb{Z}}(x) = (0)$ é ideal essencial de $\mathbb{Z}$, que não pode ocorrer pela definição de ideal essencial. Logo, $n \neq 0$.
Como $n \in An_{\mathbb{Z}}(x)$, devemos ter $xn = 0$, com $n \neq 0$. Portanto $x = 0$. Logo, $Z(\mathbb{Z}) = (0)$ e $\mathbb{Z}$ é anel não singular, isto é, (0) é ideal não singular.

■

Vamos relacionar ideais não singulares com as classes de ideais primos já estudadas anteriormente:

Proposição 2.9 *:*

a) Todo ideal fortemente primo é primo não singular.

b) Todo ideal primo não singular é primo.

Demonstração: a) Seja P um ideal fortemente primo do anel R'. Por definição $R = \dfrac{R'}{P}$ é anel fortemente primo. Pela Proposição 2.7 (a), P é ideal primo. Admita provado que $Z(R) = (0)$. Então temos que $Z\left(\dfrac{R'}{P}\right) = (0)$ e, portanto, P será ideal primo não singular. Assim, é suficiente provar que todo anel fortemente primo é não singular. Seja então R um anel fortemente primo. Suponha $Z(R) \neq (0)$. Como (0) é ideal fortemente primo de R e $Z(R)$ é ideal de R tal que $(0) \subsetneq Z(R)$, aplicamos a Proposição 2.6 para obter um conjunto finito $F = \{a_1, a_2, \ldots, a_n\} \subseteq Z(R)$ tal que $F.a = (0)$, com $a \in R$, implica $a = 0$, ou seja, $An_R(F) = (0)$. Temos que, para cada i, $An_r(a_i)$ é essencial (pois a_i está em $Z(R)$). Agora, $An_r(a_1)$ é essencial e $An_r(a_2)$ é ideal à direita, logo, $An_r(a_1) \cap An_r(a_2) \neq (0)$. Mas sabemos que intersecção de ideais à direita é ideal à direita, logo, $An_r(a_1) \cap An_r(a_2) \neq (0)$ é ideal à direita e $(An_r(a_1) \cap An_r(a_2)) \cap An_r(a_3) \neq (0)$. Repetindo os passos, teremos que $\cap_{i=1}^{n} An_r(a_i) \neq (0)$. Logo, temos que $(0) \neq \cap_{i=1}^{n} An_r(a_i) = An_r(F) = (0)$. Absurdo. Portanto, $Z(R) = (0)$.

b) Por definição.

■

Para um anel R, usaremos as seguintes notações:
. $\mathcal{C}(R)$ - para indicar o conjunto dos ideais completamente primos de R.
. $\mathcal{S}(R)$ - para indicar o conjunto dos ideais fortemente primos de R.
. $\mathcal{Z}(R)$ - para indicar o conjunto dos ideais primos não singulares de R.
. $\mathcal{P}(R)$ - para indicar o conjunto dos ideais primos de R.

De acordo com as Proposições 2.7 e 2.9 podemos concluir que:

$$\mathcal{C}(R) \subseteq \mathcal{S}(R) \subseteq \mathcal{Z}(R) \subseteq \mathcal{P}(R).$$

Cada uma das inclusões acima é estrita. Vimos no Exemplo 2.7 que $\mathcal{C}(R) \subsetneq \mathcal{S}(R)$, e, pelos comentários feitos no final da seção anterior, não é fácil obter exemplos para ver que as últimas duas inclusões acima são estritas.

2.4 Ideais Maximais, Primitivos e Primos nil semi-simples.

No Capítulo 1 vimos a definição de ideais maximais em anéis comutativos. Para anéis não comutativos a definição de ideal maximal é a mesma, como descrevemos abaixo.

Definição 2.13 : *Sejam R um anel e M um ideal de R, $M \neq R$. Dizemos que M é ideal maximal de R quando:*

$$J \textit{ ideal de } M \textit{ tal que } M \subseteq J \subseteq R \textit{ implica } J = M \textit{ ou } J = R.$$

Observação 2.5 : *Um ideal maximal à direita é definido de forma análoga à ideal maximal, simplesmente trocando ideais por ideais à direita.*

De forma análoga ao que vimos para anéis comutativos, temos que, para um anel qualquer, um ideal maximal sempre é ideal primo.

Proposição 2.10 : *Seja R um anel. Então todo ideal maximal de R é ideal primo de R.*

Demonstração: Sejam P um ideal maximal de R, A e B ideais de R tais que $AB \subseteq P$. Suponha $A \nsubseteq P$. Como $A + P$ é ideal de R temos

$$P \subsetneq A + P \subseteq R \Rightarrow A + P = R \Rightarrow 1 = a + p, \ a \in A \text{ e } p \in P.$$

Dado $b \in B$, podemos escrever $b = ab + pb$.
Como $ab \in AB \subseteq P$ e $pb \in P$, temos que $b \in P$. Logo, $B \subseteq P$ e P é ideal primo de R.

■

A Proposição 2.10 garante que o conjunto dos ideais maximais formam uma classe de ideais primos. Veremos agora uma informação mais precisa.

Proposição 2.11 : *Todo ideal maximal é ideal fortemente primo.*

Demonstração: Seja M um ideal maximal do anel R. Tomemos I ideal de R tal que $M \subsetneq I$. Então temos $I = R$. Portanto, $\{1\} \subset I$ e se $a \in R$ e $\{1\}.a \subseteq M$, então $a \in M$.
Pela Proposição 2.6, M é fortemente primo.

■

Usando a notação
. $\mathcal{M}(R)$ - para indicar o conjunto dos ideais maximais de R
temos as inclusões

$$\mathcal{M}(R) \subseteq \mathcal{S}(R) \subseteq \mathcal{Z}(R) \subseteq \mathcal{P}(R).$$

O Exemplo abaixo mostra que $\mathcal{M}(R) \subsetneqq \mathcal{S}(R)$.

Exemplo 2.11 : *Ideal fortemente primo que não é ideal maximal.*

Tome $R = \mathbb{Z}$ e $P = (0)$. Como $\mathbb{Z}$ é domínio comutativo temos que (0) é ideal completamente primo e portanto é ideal fortemente primo. Claro que (0) não é ideal maximal de $\mathbb{Z}$, pois $2.\mathbb{Z}$ é ideal de $\mathbb{Z}$ e $(0) \subsetneqq 2.\mathbb{Z} \subsetneqq \mathbb{Z}$.

■

Observe que o Exemplo 2.11 mostra algo mais. A saber, mostra que
$\mathcal{C}(R) \nsubseteq \mathcal{M}(R)$. Vejamos agora que $\mathcal{M}(R) \nsubseteq \mathcal{C}(R)$.

Exemplo 2.12 : *Ideal maximal que não é ideal completamente primo.*

Tome $R = M_2(\mathbb{Z})$ e $P = (0)$. Já vimos no Exemplo 2.1 que (0) não é ideal completamente primo. No entanto, como R é anel simples, temos que (0) é ideal maximal de R.

$\blacksquare$

Vamos ver agora, outras duas importantes classes de ideais primos.

Definição 2.14 *: Dado um ideal à direita L de R, definimos $(L : R)$ por*

$$(L : R) = \{x \in R; Rx \subseteq L\}.$$

Proposição 2.12 *: Seja L um ideal à direita do anel R.*

(a) $(L : R)$ é ideal (bilateral) de R.

(b) $(L : R) \subseteq L$

(c) $(L : R)$ é o maior ideal (bilateral) de R que está contido em L.

Demonstração: (a) Claro que $(L : R) \neq \varnothing$, pois $0 \in (L : R)$.
Sejam $x, y \in (L : R)$. Então os ideais à esquerda Rx e Ry estão contidos no ideal à direita L. Assim:
$R(x - y) \subseteq Rx - Ry \subseteq L \Rightarrow x - y \in (L : R)$.
$R(xy) = (Rx)y \subseteq Ly \subseteq L \Rightarrow xy \in (L : R)$.
Portanto, $(L : R)$ é subanel de R.
Tome agora $r \in R$.
$R(xr) = (Rx)r \subseteq Lr \subseteq L \Rightarrow xr \in (L : R)$.
$R(rx) \subseteq (Rr)x \subseteq Rx \subseteq L \Rightarrow rx \in (L : R)$.
Segue que $(L : R)$ é ideal bilateral de R.

(b) Se $x \in (L : R)$ então $Rx \subseteq L$ e, como R tem unidade, vem que $x \in L$.
Logo, $(L : R) \subseteq L$.

(c) Seja I um ideal de R tal que $I \subseteq L$. Dado $u \in I$, temos que $Ru \subseteq I \subseteq L$, ou seja, $u \in (L : R)$. Logo, $I \subseteq (L : R)$.

$\blacksquare$

Exemplo 2.13 : *Calcular* $(n\mathbb{Z} : \mathbb{Z})$ *para cada* $n \in \mathbb{N}$.

Pela Proposição anterior, $(n\mathbb{Z} : \mathbb{Z})$ é o maior ideal bilateral de $\mathbb{Z}$ contido em $n\mathbb{Z}$. Logo, $(n\mathbb{Z} : \mathbb{Z}) = n\mathbb{Z}$.

$\blacksquare$

O Exemplo 2.13 pode ser facilmente generalizado.

Exemplo 2.14 : *Se* R *é anel comutativo e* L *é ideal de* R *então* $(L : R) = L$. *E, de forma mais geral, se* R *é anel qualquer e* L *é ideal bilateral de* R *então* $(L : R) = L$.

Análogo ao Exemplo 2.13.

$\blacksquare$

O Exemplo 2.14 mostra que o conjunto $(L : R)$ só é interessante quando R é não comutativo. E, no caso não comutativo, só é interessante quando L não é ideal bilateral de R.

Exemplo 2.15 : *É fácil ver que* $L = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}) \right\}$ *é ideal à direita do anel* $R = M_2(\mathbb{R})$. *Vamos calcular* $(L : R)$.

Sabemos que $(L : R)$ é o maior ideal bilateral de R contido em L. Como R é simples e $L \neq R$, temos que $(L : R) = (0)$.

$\blacksquare$

Generalizando o Exemplo 2.15 temos:

Exemplo 2.16 : *Se* R *é um anel simples e* L *é um ideal à direita próprio de* R *então* $(L : R) = (0)$.

$\blacksquare$

Definição 2.15 : *Um ideal* P *de* R *é dito primitivo (à direita) se existir um ideal maximal à direita* L *de* R *tal que* $(L : R) = P$.

Definição 2.16 : *Um anel* R *é dito primitivo (à direita) se* (0) *é um ideal primitivo.*

Proposição 2.13 : *Seja P um ideal de R. São equivalentes.*

(i) P é ideal primitivo de R.

(ii) $\dfrac{R}{P}$ é anel primitivo.

Demonstração: Em vários lugares nesta demonstração usaremos, sem mencionar, o Segundo Teorema do Homomorfismo e seu Corolário para ideais à direita, como provados no Capítulo 1.

$(i) \Rightarrow (ii)$ Por hipótese, existe um ideal à direita maximal L de R tal que $(L : R) = P$. Pela Proposição 2.12 (b), temos que $(L : R) \subseteq L$ e, então, $P \subseteq L$. Segue que $\dfrac{L}{P}$ é ideal à direita do anel $\dfrac{R}{P}$. Vamos provar que $\dfrac{L}{P}$ é ideal à direita maximal de $\dfrac{R}{P}$.

Seja $\widehat{J}$ um ideal à direita de $\dfrac{R}{P}$ tal que $\dfrac{L}{P} \subseteq \widehat{J} \subseteq \dfrac{R}{P}$. Então $\widehat{J} = \dfrac{J}{P}$ para algum ideal à direita J de R tal que $P \subseteq J$. Assim:

$$\frac{L}{P} \subseteq \frac{J}{P} \subseteq \frac{R}{P} \Rightarrow L \subseteq J \subseteq R \Rightarrow J = L \text{ ou } J = R \Rightarrow \widehat{J} = \frac{L}{P} \text{ ou } \widehat{J} = \frac{R}{P}.$$

Portanto, $\dfrac{L}{P}$ é ideal à direita maximal de $\dfrac{R}{P}$.

Seja $\overline{u} \in \left(\dfrac{L}{P} : \dfrac{R}{P}\right)$. Então $\dfrac{R}{P}\overline{u} \subseteq \dfrac{L}{P}$ e, daí, $Ru \subseteq L$. Isso diz que $u \in (L : R) = P$ e, portanto, $\overline{u} = \overline{0}$. Assim, temos provado que $\left(\dfrac{L}{P} : \dfrac{R}{P}\right) = (\overline{0})$ e $(\overline{0})$ é ideal primitivo de $\dfrac{R}{P}$. Logo, $\dfrac{R}{P}$ é anel primitivo.

$(ii) \Rightarrow (i)$ Por hipótese, existe ideal à direita maximal $\dfrac{L}{P}$ de $\dfrac{R}{P}$ tal que $\left(\dfrac{L}{P} : \dfrac{R}{P}\right) = (\overline{0})$. Então L é ideal à direita de R que contém P. Seja J ideal à direita de R tal que $L \subseteq J \subseteq R$. Então $\dfrac{J}{P}$ é ideal à direita de $\dfrac{R}{P}$ e $\dfrac{L}{P} \subseteq \dfrac{J}{P} \subseteq \dfrac{R}{P}$. Pela maximalidade de $\dfrac{L}{P}$, temos $\dfrac{J}{P} = \dfrac{L}{P}$ ou $\dfrac{J}{P} = \dfrac{R}{P}$ e, daí, $J = L$ ou $J = R$. Segue que L é ideal à direita maximal de R.

Sabemos, pela Proposição 2.12 (c), que $(L : R)$ é o maior ideal bilateral de R contido em L. Como P é ideal bilateral de R e $P \subseteq L$, temos que $P \subseteq (L : R)$. Tome agora $u \in (L : R)$. Então $Ru \subseteq L$ e daí $\dfrac{R}{P}\overline{u} \subseteq \dfrac{L}{P}$. Segue que $\overline{u} \in \left(\dfrac{L}{P} : \dfrac{R}{P}\right) = (\overline{0})$, isto é,

$u \in P$. Portanto, $(L : R) = P$ e P é ideal primitivo de R.

■

A proposição abaixo mostra que, no caso comutativo, os anéis primitivos são exatamente os corpos.

Proposição 2.14 : *Seja R um anel comutativo. São equivalentes:*

(i) R é corpo

(ii) R é anel primitivo.

Demonstração: Lembre que pela Proposição 1.8 temos que R é corpo se, e somente se, (0) é ideal maximal de R.

$(i) \Rightarrow (ii)$ Basta provar que $((0) : R) = (0)$. Como R é anel simples, isso segue do Exemplo 2.16.

$(ii) \Rightarrow (i)$ Por hipótese existe um ideal maximal L de R tal que $(L : R) = (0)$. Pela Proposição 2.12 (c), (0) é o maior ideal contido em L. Logo, $L = (0)$ é ideal maximal de R e, portanto, R é corpo.

■

Exemplo 2.17 : *Todo anel simples é primitivo.*

Seja R um anel simples e L um ideal à direita maximal de R, que existe conforme vimos na Observação 1.7. Pela Proposição 2.12 (c), $(L : R)$ é o maior ideal bilateral de R contido em L. Como R é simples e $L \neq R$, a única possibilidade é $(L : R) = (0)$. Logo, (0) é ideal primitivo de R e então R é anel primitivo.

■

Proposição 2.15 : *Todo ideal maximal é ideal primitivo.*

Demonstração: Seja M um ideal maximal do anel R. Note que o anel $\dfrac{R}{M}$ é simples. De fato, pelo Segundo Teorema do Homomorfismo um ideal de $\dfrac{R}{M}$ deve ser da forma $\dfrac{I}{M}$ onde I é ideal de R e $M \subseteq I \subseteq R$. Pela maximalidade de M, vem que $I = M$ ou

$I = R$. Assim, $\dfrac{I}{M}$ é ideal trivial e $\dfrac{R}{M}$ é anel simples.

O Exemplo 2.17 garante que $\dfrac{R}{M}$ é anel primitivo, e a Proposição 2.13 diz que M é ideal primitivo de R.

$\blacksquare$

Notação:

- $p(R)$ - indica o conjunto dos ideais primitivos de R.

Pela Proposição 2.15, temos que

$$\mathcal{M}(R) \subseteq p(R).$$

Para apresentar nossa última classe de ideais primos definimos inicialmente os ideais que são nil ideais.

Definição 2.17 : *Um ideal I do anel R é um nil ideal se cada $x \in I$ é um elemento nilpotente, isto é, existe $n \geq 1$ tal que $x^n = 0$.*

Definição 2.18 : *Um ideal primo P do anel R é dito nil semi-simples se o anel $\dfrac{R}{P}$ não possui nil ideais não nulos.*

O lema a seguir será útil para relacionar ideais nil semi-simples com ideais primitivos.

Lema 2.2 : *Sejam R um anel e L um ideal à direita de R.*

(a) Se $c \in R$ é nilpotente então $1 - c$ é inversível em R.

(b) Se $(L : R) = (0)$ e B é ideal de R contido em L então $B = (0)$.

Demonstração: (a) $c^n = 0 \Leftrightarrow c^n - 1 = -1 \Leftrightarrow (c-1)(c^{n+1} + ... + 1) = -1 \Leftrightarrow (1-c)(c^{n+1} + ... + 1) = 1$.
Ou seja, $1 - c$ é inversível.

(b) Pela Proposição 2.12 (c), $(L : R)$ é o maior ideal bilateral contido em L. Como B é ideal de R e $B \subseteq L$, temos que $B \subseteq (L : R) = (0)$.

$\blacksquare$

Proposição 2.16 : *Todo ideal primitivo é primo nil semi-simples.*

Demonstração: Seja P um ideal primitivo do anel R'. Pela Proposição 2.13, $R = \dfrac{R'}{P}$ é anel primitivo. Admita provado que $(\overline{0})$ é ideal primo nil semi-simples de R.
Pelo fato de $(\overline{0})$ ser ideal primo de $\dfrac{R'}{P} = R$, vem que $\dfrac{R'}{P}$ é anel primo, e então P é ideal primo.

Pelo fato de (0) ser ideal nil semi-simples de $R = \dfrac{R'}{P}$, temos, por definição, que $\dfrac{R}{(0)} = \dfrac{R'}{P}$ não possui nil ideais. Assim, P é ideal nil semi-simples de R.
Portanto, nossa prova ficará completa quando mostrarmos que para um anel qualquer R vale:

$$R \text{ anel primitivo} \Rightarrow (0) \text{ é ideal primo nil semi-simples de } R.$$

Como R é primitivo, existe um ideal maximal à direita L tal que $(L : R) = (0)$. Sejam A e B ideais de R tais que $AB = (0)$ e $A \neq (0)$. Pelo Lema 2.2 (b), temos que $A \nsubseteq L$. Então, $L \subsetneq A + L \subseteq R$ e, como L é maximal à direita, vem que $A + L = R$ e, daí, existem $a \in A$, $x \in L$ tais que $a + x = 1$.
Então, para cada $b \in B$, temos $b = ab + xb = xb \in L$, pois $AB = (0)$. Portanto, $B \subseteq L$ e, como $(L : R) = (0)$, segue do Lema 2.2 (b) que $B = (0)$. Assim, R é anel primo, isto é, (0) é ideal primo de R.
Seja agora I um nil ideal de R. Se $I \neq (0)$, então $I \nsubseteq L$ pelo Lema 2.2 (b). Logo, $L \subsetneq I + L \subseteq R$, o que implica $I + L = R$. Daí, existem $c \in I$ e $y \in L$ tais que $c + y = 1$. Portanto, $y = 1 - c$ é inversível em R, já que c é nilpotente. Logo, existe $t \in R$ tal que $yt = 1$. Como $y \in L$, $yt \in L$, e, portanto, $1 \in L$. Logo, L=R, o que é um absurdo, pois L é maximal à direita.
Portanto R não possui nil ideais não nulos, isto é, (0) é ideal nil semi-simples de R.

$\blacksquare$

Exemplo 2.18 : *Ideal primo nil semi-simples que não é primitivo.*

Tome $P = (0)$ no anel $R = \mathbb{Z}$. De acordo com a Proposição 2.14, $\mathbb{Z}$ não é anel primitivo e então $P = (0)$ não é ideal primitivo.

Por outro lado, como $\mathbb{Z}$ é domínio temos que $P = (0)$ é ideal primo.
Para ver que $P = (0)$ é nil semi-simples devemos verificar que $\dfrac{\mathbb{Z}}{(0)} = \mathbb{Z}$ não tem nil ideal não nulo. Mas isso é claro pois $\mathbb{Z}$ é domínio.

$\blacksquare$

Notação:

. $\mathcal{N}(R)$ - indica o conjunto dos ideais primos nil semi-simples de R.

Verificamos neste capítulo que:

$$\begin{array}{ccccccc} \mathcal{C}(R) & \subseteq & \mathcal{S}(R) & \subseteq & \mathcal{Z}(R) & \subseteq & \mathcal{P}(R) \\ & & \cup\!| & & & & \cup\!| \\ & & \mathcal{M}(R) & \subseteq & p(R) & \subseteq & \mathcal{N}(R) \end{array}$$

Seja $f : A \to B$ um isomorfismo de anéis. O Segundo Teorema do Homomorfismo assegura que a correspondência $J \mapsto f(J)$, entre ideais à direita (à esquerda ou bilaterais) de A e ideais à direita (à esquerda ou bilaterais) de $B = f(A)$, é biunívoca e preserva a inclusão.

Agora, vamos mostrar que essa correspondência preserva cada uma das classes de ideais estudados até o momento. De outra forma: mostraremos que cada uma das classes de ideais que listamos é invariante por isomorfismo. Este resultado será usado no Capítulo 3.

Proposição 2.17 : *Seja $f : A \to B$ um isomorfismo de anéis.*

(a) P é ideal completamente primo de $A \Leftrightarrow f(P)$ é ideal completamente primo de B.

(b) P é ideal primo de $A \Leftrightarrow f(P)$ é ideal primo de B.

(c) P é ideal à direita (à esquerda ou bilateral) maximal de $A \Leftrightarrow f(P)$ é ideal à direita (à esquerda ou bilateral) maximal de B.

(d) P é ideal primitivo de $A \Leftrightarrow f(P)$ é ideal primitivo de B.

(e) P é ideal fortemente primo de $A \Leftrightarrow f(P)$ é ideal fortemente primo de B.

(f) P é ideal primo não singular de $A \Leftrightarrow f(P)$ é ideal primo não singular de B.

(g) P é ideal primo nil semi-simples de $A \Leftrightarrow f(P)$ é ideal primo nil semi-simples de B.

Demonstração: É claro que, em cada item, basta provar a direção $\Rightarrow$, pois na direção $\Leftarrow$ basta usar f^{-1}.

(a) Sejam $x, y \in B$ tais que $xy \in f(P)$. Então $x = f(a)$ e $y = f(b)$, com $a, b \in A$.

$$\begin{aligned} f(ab) = f(a)f(b) = xy \in f(P) \Rightarrow ab \in P \Rightarrow a \in P \text{ ou } b \in P \\ \Rightarrow x = f(a) \in f(P) \text{ ou } y = f(b) \in f(P). \end{aligned}$$

Portanto, $f(P)$ é ideal completamente primo de B.

(b) Para provar que $f(P)$ é ideal primo de B, vamos usar a Proposição 2.2 ((iii)). Sejam $x, y \in B$ tais que $xBy \subseteq f(P)$. Devemos provar que $x \in f(P)$ ou $y \in f(P)$. Escreva $x = f(a), y = f(b)$, com $a, b \in A$. Para cada $c \in A$, temos $f(c) \in B$ e então $xf(c)y \in xBy \subseteq f(P)$. Segue que:

$$f(acb) = f(a)f(c)f(b) = xf(c)y \in f(P) \Rightarrow acb \in P.$$

Logo, $aAb \subseteq P$ e, como P é ideal primo de A, temos que $a \in P$ ou $b \in P$. Assim, $x = f(a) \in f(P)$ ou $y = f(b) \in f(P)$. Portanto, $f(P)$ é ideal primo de B.

(c) Faremos para ideais à direita maximais. Os outros casos são análogos.
Seja J ideal à direita de B tal que $f(P) \subseteq J \subseteq B$. Sabemos, pelo Segundo Teorema do Homomorfismo, que $J = f(I)$ para algum ideal à direita I de A tal que $P \subseteq I \subseteq A$. Como P é ideal à direita maximal, vem que $I = P$ ou $I = A$. Portanto, $J = f(P)$ ou $J = f(A) = B$, isto é, $f(P)$ é ideal à direita maximal de B.

(d) Usaremos a Proposição 2.12 (c).
Por hipótese, existe um ideal à direita maximal L de A tal que $(L : A) = P$. Pela Proposição 2.12 (c), temos que P é o maior ideal bilateral de A contido em L. Pelo item (c), temos que $f(L)$ é ideal à direita maximal de B. Claro que $f(P)$ é ideal bilateral de B contido em $f(L)$. Pela Proposição 2.12 (c), basta provar que $f(P)$ é o maior ideal bilateral de B contido em $f(L)$, e teremos $(f(L) : B) = f(P)$, isto é, $f(P)$ é ideal primitivo de B.
Seja então J um ideal bilateral de B tal que $J \subseteq f(L)$. Sabemos que $J = f(I)$ para

algum ideal bilateral I de A. Aplicando f^{-1} em $f(I) \subseteq f(L)$, concluímos que $I \subseteq L$. Então $I \subseteq P$ e, daí, $J = f(I) \subseteq f(P)$.

(e) Usaremos a Proposição 2.6.
Seja J ideal de B tal que $f(P) \subset J$. Sabemos que $J = f(I)$ para algum ideal I de A que contém propriamente P. Pela Proposição 2.6, existe um conjunto finito $F \subseteq I$ tal que:

$$a \in A \text{ e } Fa \subseteq P \Rightarrow a \in P.$$

Tome $\widehat{F} = f(F) \subseteq f(I) = J$, que é finito. Devemos mostrar que:

$$x \in B \text{ e } \widehat{F}x \subseteq f(P) \Rightarrow x \in f(P).$$

Escreva $x = f(a), a \in A$. Dado $u \in F$, temos $f(u) \in \widehat{F}$. Então:

$$f(u)f(a) \in \widehat{F}x \subseteq f(P) \Rightarrow f(ua) \in f(P) \Rightarrow ua \in P.$$

Segue que $Fa \subseteq P$ e, então, $a \in P$. Portanto, $x = f(a) \in f(P)$.

(f) Já sabemos por (a) que $f(P)$ é ideal primo de B. Então, pela definição de ideal primo não singular, devemos provar que $Z\left(\dfrac{B}{f(P)}\right) = (\overline{0})$. Como P é ideal primo não singular de A, temos que $Z\left(\dfrac{A}{P}\right) = (\overline{0})$.
Seja $\overline{x} = x + f(P) \in Z\left(\dfrac{B}{f(P)}\right)$. Por definição, vem que $An_{\frac{B}{f(P)}}(\overline{x})$ é ideal essencial de $\dfrac{B}{f(P)}$. Como $x \in B$, temos $a \in A$ tal que $f(a) = x$. Assim, $\overline{a} \in \dfrac{A}{P}$. Vamos mostrar que $\overline{a} \in Z\left(\dfrac{A}{P}\right)$. Para isso, temos que verificar que $An_{\frac{A}{P}}(\overline{a})$ é ideal essencial de $\dfrac{A}{P}$.
Seja então $\dfrac{I}{P}$ ideal à direita não nulo de $\dfrac{A}{P}$. Segue que I é ideal à direita de A e $P \subsetneqq I$. Aplicando f, vem que $f(P) \subsetneqq f(I) = J$ e J é ideal à direita de B. Assim, $\dfrac{J}{f(P)}$ é ideal não nulo de $\dfrac{B}{f(P)}$ e, como $An_{\frac{B}{f(P)}}(\overline{x})$ é ideal essencial de $\dfrac{B}{f(P)}$, existe $\overline{0} \neq \overline{u} \in \dfrac{J}{f(P)} \cap An_{\frac{B}{f(P)}}$, isto é, $\overline{0} \neq \overline{u} \in \dfrac{J}{f(P)}$ e $\overline{x}.\overline{u} = \overline{0}$. Note que $\overline{u} = u + f(P)$ com

$u \in J = f(I)$, e de $\overline{x}.\overline{u} = \overline{0}$ temos $xu \in f(P)$. Podemos escrever $u = f(v), v \in I$.

$$xu \in f(P) \Rightarrow f(a)f(v) \in f(P) \Rightarrow f(av) \in f(P) \Rightarrow av \in P \Rightarrow \overline{a}.\overline{v} = \overline{0} \text{ em } \frac{A}{P}.$$

Além disso, $\overline{u} \neq \overline{0}$ implica em $u \notin f(P)$ e daí $v \notin P$.
Segue que $\overline{v} \neq \overline{0}, \overline{v} \in \dfrac{I}{P} \cap An_{\frac{A}{P}}(\overline{a})$. Portanto, $An_{\frac{A}{P}}(\overline{a})$ é ideal essencial de $\dfrac{A}{P}$ e então $\overline{a} \in Z\left(\dfrac{A}{P}\right) = (\overline{0})$. Agora podemos concluir que $a \in P$. Mas $a = f^{-1}(x) \in P$ e, daí, $x \in f(P)$. Logo, $\overline{x} = x + f(P) = \overline{0}$. Provamos assim que $Z\left(\dfrac{B}{f(P)}\right) = (\overline{0})$.

(g) Pelo item (a), já sabemos que $f(P)$ é ideal primo de B. Então, pela definição de ideal primo nil semi-simples, devemos mostrar que $\dfrac{B}{f(P)}$ não possui nil ideal não nulo.
Seja $\dfrac{J}{f(P)}$ nil ideal de $\dfrac{B}{f(P)}$. Segue que J é ideal de B e, portanto, $J = f(I)$ para algum ideal I de A que contém P. Vamos mostrar que $\dfrac{I}{P}$ é nil ideal de $\dfrac{A}{P}$. De fato, dado $\overline{v} = v + P \in \dfrac{I}{P}$, com $v \in I$, temos que $f(v) \in J$. Assim, $\overline{f(v)} = f(v) + f(P) \in \dfrac{J}{f(P)}$ que é nil ideal. Logo, existe $n \in \mathbb{N}^*$ tal que $\left(\overline{f(v)}\right)^n = \overline{0}$. Isso diz que $\overline{f(v^n)} = \overline{0}$, isto é, $f(v^n) \in f(P)$.
Segue que $v^n \in P$ e, daí, $\overline{0} = \overline{v^n} = (\overline{v})^n$. Concluímos que $\overline{v}$ é nilpotente e, então, $\dfrac{I}{P}$ é nil ideal de $\dfrac{A}{P}$.
Por hipótese, P é ideal primo nil semi-simples de A, ou seja, $\dfrac{A}{P}$ não possui nil ideal não nulo. Assim, $\dfrac{I}{P} = (\overline{0})$, que leva a $I = P$. Aplicando f, temos $J = f(I) = f(P)$ e, então, $\dfrac{J}{f(P)} = (\overline{0})$. Portanto, $\dfrac{B}{f(P)}$ não possui nil ideal não nulo.

$\blacksquare$

3 Radicais de Anéis

Quando estudamos um anel R, algumas vezes é conveniente cancelar elementos cujo comportamento é indesejável. Fazemos isso agrupando esses elementos num ideal $\alpha(R)$ de R e estudando o anel $\dfrac{R}{\alpha(R)}$, definindo $\alpha(R)$ de modo que $\alpha\left(\dfrac{R}{\alpha(R)}\right) = (0)$. Este ideal $\alpha(R)$ será chamado Radical de R.

Neste Capítulo vamos apresentar os principais radicais estudados na matemática. A saber, o radical primo, radical de Jacobson, nil radical superior, nil radical generalizado, radical fortemente primo, radical singular e o radical de Brown-McCoy.

Nosso objetivo é verificar que cada um destes radicais pode ser obtido como intersecção de alguma das classes de ideais primos estudadas no Capítulo 2.

Exemplo 3.1 *: Seja R um anel comutativo. Então $Nil(R)$, que é o conjunto dos elementos nilpotentes de R, é um radical de R.*

$Nil(R)$ **é ideal de** R**:** Sejam $x, y \in Nil(R)$. Portanto, existem n, $m \in \mathbb{N}$ tal que $x^n = 0, y^m = 0$. Então:

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} \left(\begin{array}{c} n+m \\ k \end{array} \right) x^{n+m-k}(-y)^k.$$

Mas x^{n+m-k} só será diferente de zero quando $k < m$, e daí, $(-y)^k = 0$. Logo, $x - y$ é nilpotente.
Agora tome $x \in Nil(R)$ e $a \in R$. Então, existe $n \in \mathbb{N}$ tal que $x^n = 0$. Logo:
$(x.a)^n = (a.x)^n = a^n x^n = a^n.0 = 0$, ou seja, $a.x$ e $x.a$ são nilpotentes.

$Nil\left(\dfrac{R}{Nil(R)}\right) = (0)$**:** Seja $\overline{x} \in Nil\left(\dfrac{R}{Nil(R)}\right)$. Então existe n tal que $(\overline{x})^n = \overline{0}$. Assim:

$$(\overline{x})^n = \overline{0} \Rightarrow \overline{x^n} = \overline{0} \Rightarrow x^n \in Nil(R) \Rightarrow \exists m \in \mathbb{N}\ talque\ (x^n)^m = 0$$
$$\Rightarrow x^{nm} = 0 \Rightarrow x \in Nil(R) \Rightarrow \overline{x} = \overline{0}.$$

■

Portanto, $Nil(R)$ é um radical de R, chamado nil radical de R. Como o anel $\dfrac{R}{Nil(R)}$ não possui elementos nilpotentes, pode ser mais útil estudá-lo do que estudar o anel R.

Observação 3.1 : *Veremos adiante o nil radical superior, em um anel R qualquer. Esse também será denotado por $Nil(R)$ e, no caso em que R é comutativo, coincide com o radical visto no Exemplo 3.1.*

Vamos então, definir alguns radicais importantes.

Notação:

- $\beta(R)$ - indica a intersecção de todos os ideais primos de R.

Nosso objetivo é mostrar que $\beta(R)$ é um radical. Claro que $\beta(R)$ é ideal de R, e $\beta(R)$ está contido em todo ideal primo P de R. Falta mostrar que $\beta\left(\dfrac{R}{\beta(R)}\right) = 0$. Para isso usaremos o lema abaixo.

Lema 3.1 : *Se P é ideal primo de R então $\dfrac{P}{\beta(R)}$ é ideal primo de $\dfrac{R}{\beta(R)}$.*

Demonstração: Como P é ideal de R e $\beta(R) \subseteq P$, é claro que $\dfrac{P}{\beta(R)}$ é ideal de $\dfrac{R}{\beta(R)}$. Assim, temos o anel quociente $\dfrac{\frac{R}{\beta(R)}}{\frac{P}{\beta(R)}}$, que vimos, no Exemplo 1.15, ser isomorfo a $\dfrac{R}{P}$. Como P é ideal primo de R temos que $\dfrac{R}{P}$ é anel primo, isto é, (0) é ideal primo de $\dfrac{R}{P}$. Pelo isomorfismo, concluímos que $(\overline{0}) = \dfrac{P}{\beta(R)}$ é ideal primo de $\dfrac{R}{\beta(R)}$.

■

Observação 3.2 : *Uma alternativa para provar o Lema 3.1 sem trabalhar via isomorfismo é a seguinte: Sejam $\widehat{A}$ e $\widehat{B}$ ideais de $\dfrac{R}{\beta(R)}$ tais que $\widehat{A}\widehat{B} \subseteq \dfrac{P}{\beta(R)}$. Pelo Segundo Teorema do Homomorfismo, $\widehat{A} = \dfrac{A}{\beta(R)}$ e $\widehat{B} = \dfrac{B}{\beta(R)}$ em que A e B*

são ideais de R que contêm $\beta(R)$. Agora, usando o fato de P ser ideal primo de R, temos:

$$\widehat{A}\widehat{B} \subseteq \frac{P}{\beta(R)} \Rightarrow \frac{A}{\beta(R)}\frac{B}{\beta(R)} \subseteq \frac{P}{\beta(R)} \Rightarrow AB \subseteq P \Rightarrow A \subseteq P \text{ ou } B \subseteq P$$
$$\Rightarrow \widehat{A} = \frac{A}{\beta(R)} \subseteq \frac{P}{\beta(R)} \text{ ou } \widehat{B} = \frac{B}{\beta(R)} \subseteq \frac{P}{\beta(R)}.$$

Logo, $\dfrac{P}{\beta(R)}$ é ideal primo de $\dfrac{R}{\beta(R)}$.

Proposição 3.1 *: $\beta(R)$ é um radical.*

Demonstração: Basta provar que $\beta\left(\dfrac{R}{\beta(R)}\right) = (\overline{0})$.

Seja $\overline{x} = x + \beta(R) \in \beta\left(\dfrac{R}{\beta(R)}\right)$. Tomemos P ideal primo de R. Pelo Lema 3.1 $\dfrac{P}{\beta(R)}$ é ideal primo de $\dfrac{R}{\beta(R)}$. Portanto, $\overline{x} \in \dfrac{P}{\beta(R)}$ e, daí $x \in P$. Então, x está na intersecção de todos os ideais primos de R, ou seja, $x \in \beta(R)$. Logo, $\overline{x} = \overline{0}$.

■

Definição 3.1 *: O radical $\beta(R)$ é chamado radical primo ou nil radical inferior do anel R.*

O radical primo pode ser caracterizado através de outro tipo de ideais, chamados ideais semiprimos. Trataremos disso agora.

Definição 3.2 *: Um ideal I de R é dito nilpotente se existir $n \geq 1$ tal que $I^n = 0$.*

Definição 3.3 *: Um ideal L de R é dito semiprimo se $L \neq R$ e*

$$aRa \subseteq L, a \in R \Rightarrow a \in L.$$

Definição 3.4 *: O anel R é semiprimo se o ideal (0) é semiprimo.*

Com essas definições, temos a seguinte

Proposição 3.2 *: São equivalentes:*

(i) *L é um ideal semiprimo de R.*

(ii) $\dfrac{R}{L}$ *não possui ideais nilpotentes não triviais.*

(iii) *L é intersecção de ideais primos.*

Demonstração: $(i) \Rightarrow (ii)$ Suponha que $\dfrac{R}{L}$ tenha um ideal nilpotente não trivial I. Então, existe $n \in \mathbb{N}^*$ tal que $I^n = (0)$ e $I^{n-1} \neq (0)$ (pois $I \neq (0)$). Tomando $H = I^{n-1}$ vem que $H \neq (0)$ e $H^2 = (0)$. Desde que H é ideal de $\dfrac{R}{L}$ segue do Segundo Teorema do Homomorfismo que $H = \dfrac{J}{L}$, para algum ideal J de R tal que $L \subseteq J$. Então:

$$H \neq (0) \Rightarrow L \subsetneq J \Rightarrow \exists a \in J \backslash L \Rightarrow \overline{0} \neq \overline{a} \in \frac{J}{L} \Rightarrow \overline{a}\frac{R}{L}\overline{a} \subseteq H^2 = \{\overline{0}\}.$$

Seja $r \in R$. Então $\overline{ara} = \overline{0}$ e daí $aRa \subseteq L$. Porém, $a \notin L$. Isso contradiz a hipótese (i) que assegura que L é ideal semi-primo de R. Portanto, $\dfrac{R}{L}$ não tem ideal nilpotente não trivial.

$(ii) \Rightarrow (i)$ Seja $a \in R$ tal que $aRa \subseteq L$. Então, como $R^2 = R$ (pois R tem unidade), $(RaR)^2 = RaRaR \subseteq L$.

Segue que $\left(\dfrac{R}{L}\overline{a}\dfrac{R}{L}\right)^2 = (\overline{0})$. Em particular, $\overline{a} = \overline{0}$ e, daí, $a \in L$. Portanto, L é ideal semi-primo de R.

$(i) \Rightarrow (iii)$ Seja $\{P_i; i \in \Gamma\}$ o conjunto dos ideais primos de R que contêm L. Como $L \neq R$, temos, pela Proposição 1.6, que existe um ideal maximal M de R tal que $L \subseteq M$. Mas, então, M é primo e, portanto, $\{P_i; i \in \Gamma\} \neq \emptyset$. Seja $H = \cap_{i\in\Gamma} P_i$. Claro que $L \subseteq H$. Agora, suponha que exista $a_0 \in H \backslash L$. Então, pela caracterização de ideais primos vista na Proposição 2.2 (iii) temos:

$$a_0 \notin L \text{ e } L \text{ ideal primo de } R \Rightarrow a_0Ra_0 \nsubseteq L \Rightarrow \exists r_1 \in R \text{ tal que } a_0r_1a_0 = a_1 \notin L,$$
$$a_1 \notin L \text{ e } L \text{ ideal primo de } R \Rightarrow a_1Ra_1 \nsubseteq L \Rightarrow \exists r_2 \in R \text{ tal que } a_1r_2a_1 = a_2 \notin L.$$

Por indução, construímos uma seqüência $S = \{a_0, a_1, a_2, \ldots\}$ tal que para cada $i \in \mathbb{N}^*$ existe $r_i \in R$ que satisfaz $a_i = a_{i-1}r_ia_{i-1} \notin L$.

Seja $\Im = \{J; J \text{ é ideal de } R, L \subseteq J \text{ e } J \cap S = \emptyset\}$ ordenado por inclusão. Note que

$\Im \neq \emptyset$ pois $L \in \Im$.
Dada uma cadeia $\{J_\lambda\}_{\lambda\in\Omega}$ em $\Im$ temos que $J = \cup_{\lambda\in\Omega} J_\lambda$ é ideal de R, já que $\{J_\lambda\}_{\lambda\in\Omega}$ é totalmente ordenado. Claro que $L \subseteq J$ e $J \cap S = \emptyset$. Logo J é cota superior em $\Im$ para $\{J_\lambda\}_{\lambda\in\Omega}$. Pelo Lema de Zorn, existe um elemento maximal $P \in \Im$.

Afirmação: P é ideal primo de R.
De fato, como $P \in \Im$ sabemos que P é ideal de R. Sejam A e B ideais de R tais que $P \subset A$ e $P \subset B$. Claro que $L \subset A$ e $L \subset B$. Desde que P é maximal em $\Im$ devemos ter $A, B \notin \Im$. Então só resta $A \cap S \neq \emptyset$ e $B \cap S \neq \emptyset$. Assim existem $a_i, a_j \in S$ tais que $a_i \in A$ e $a_j \in B$. Sem perda de generalidade, assuma que $i \geq j$. Agora, note que

$$a_{i+1} = a_i r_{i+1} a_i = a_i r_{i+1} a_{i-1} r_i a_{i-1} = \ldots = a_i r_{i+1} a_{i-1} r_i a_{i-1} \ldots a_j r_{j+1} a_j \in AB$$

Mas $a_{i+1} \notin P$ e, então, $AB \nsubseteq P$. Portanto, pela Proposição 2.2 (v), vem que P é ideal primo.
Obtivemos que $a_0 \notin P$, P ideal primo que contém L. Isso leva a contradição $a_0 \notin H$, pois $P \in \{P_i; i \in \Gamma\}$. Portanto, $H \subseteq L$, e concluímos que $H = L$, ou seja, L é a intersecção de todos os ideais primos de R que o contêm.

$(iii) \Rightarrow (i)$ Por hipótese, $L = \cap_{i\in\Omega} P_i, \{P_i; i \in \Omega\}$ é conjunto de ideais primos de R. Desde que ideal primo é próprio, temos que $L \neq R$. Seja agora $a \in R$ tal que $aRa \subseteq L$. Então, para todo $i \in \Omega$ temos $aRa \subseteq P_i$. Como P_i é ideal primo, segue da Proposição 2.2 (iii), que $a \in P_i$. Portanto, $a \in L$ e L é ideal semiprimo de R.

■

Dessa proposição, temos a seguinte caracterização para $\beta(R)$:

Corolário 3.1 : *O radical primo $\beta(R)$ é o menor ideal semiprimo de R.*

Demonstração: Como todo ideal semiprimo é intersecção de ideais primos e $\beta(R)$ é intersecção de todos ideais primos de R, obviamente $\beta(R)$ é o menor ideal semiprimo.

■

Notação:
. $J(R)$ - indica a intersecção dos ideais primitivos de R.

De forma análoga ao que fizemos com $\beta(R)$, vamos provar que $J(R)$ é um radical de R. Claro que $J(R)$ é ideal de R e $J(R)$ está contido em todo ideal primitivo de R.

Proposição 3.3 : *$J(R)$ é um radical.*

Demonstração: Devemos provar que $J\left(\frac{R}{J(R)}\right) = \{\overline{0}\}$.

Tome $\overline{x} = x + J(R) \in J\left(\frac{R}{J(R)}\right)$. Então $\overline{x}$ está em todo ideal primitivo de $\frac{R}{J(R)}$.

Seja P um ideal primitivo de R. Então $J(R) \subseteq P$ e $\frac{R}{P}$ é anel primitivo pela Proposição 2.13. Vimos no Exemplo 1.15 que $\dfrac{\frac{R}{J(R)}}{\frac{P}{J(R)}} \simeq \frac{R}{P}$ e então $\dfrac{\frac{R}{J(R)}}{\frac{P}{J(R)}}$ é anel primitivo. Novamente, pela Proposição 2.13, concluímos que $\frac{P}{J(R)}$ é ideal primitivo de $\frac{R}{J(R)}$. Segue que $\overline{x} = x + J(R) \in \frac{P}{J(R)}$ e então $x \in P$.

Concluímos que $x \in P$, para todo ideal primitivo P de R, isto é, $x \in J(R)$. Logo, $\overline{x} = x + J(R) = \overline{0}$ e, portanto, $J\left(\frac{R}{J(R)}\right) = \{\overline{0}\}$.

∎

Definição 3.5 : *O radical $J(R)$ é chamado radical de Jacobson do anel R.*

O radical de Jacobson é o radical mais importante de um anel. Vejamos algumas propriedades deste radical.

Proposição 3.4 : *O radical de Jacobson $J(R)$ é igual à intersecção dos ideais maximais à direita de R.*

Demonstração: Chame $\mathcal{D}(R)$ a intersecção dos ideais à direita maximais do anel R. Devemos mostrar que $J(R) = \mathcal{D}(R)$.

"$\subseteq$": Seja $x \in J(R)$. Então x está em todo ideal primitivo de R. Se L é um ideal à direita maximal de R então $(L : R)$ é primitivo por definição. Logo $x \in (L : R)$ e daí $Rx \subseteq L$. Como R tem unidade vem que $x \in L$.

Portanto, x está em todo ideal à direita maximal de R, isto é, $J(R) \subseteq \mathcal{D}(R)$.

" $\supseteq$ ": Para cada ideal primitivo P de R, por definição, temos associado um ideal à direita maximal L_P de R tal que $(L_P : R) = P$. Além disso, pela Proposição 2.12 (b) sabemos que $P = (L_P : R) \subseteq L_P$. Segue que

$$\begin{aligned} p(R) &= \{P;\ P \text{ é ideal primitivo de } R\} \\ &\subseteq \{L_P;\ L_P \text{ é ideal à direita maximal associado à um primitivo}\} \\ &\subseteq \{L;\ L \text{ é ideal à direita maximal}\}. \end{aligned}$$

Tomando intersecções destas famílias de ideais, as inclusões acima se revertem, e então $\mathcal{D}(R) \subseteq J(R)$.

■

Uma técnica idêntica a que usamos na última parte da demonstração acima prova que $J(R)$ está contido na intersecção dos ideais maximais de R. De fato, vimos no Capítulo 2 que

$$\mathcal{M}(R) \subseteq p(R).$$

Tomando intersecções temos que $J(R) \subseteq \cap\{P;\ P \in \mathcal{M}(R)\}$.

Observação 3.3 : *Quando trabalhamos com anéis comutativos vale a igualdade acima, isto é, define-se $J(R)$ como a intersecção dos ideais maximais de R. Note que isso é uma simples conseqüência da Proposição 3.4*

Podemos também caracterizar o radical de Jacobson da seguinte maneira:

Proposição 3.5 : *(i) $x \in J(R) \Leftrightarrow 1 - xy$ é inversível à direita, para todo $y \in R$.*
(ii) O radical $J(R)$ é o maior ideal de R tal que para cada $x \in J(R)$, $1-x$ é inversível em R.

Demonstração: $(i)(\Rightarrow)$ Seja $x \in J(R)$. Suponha que $1 - xy$ não seja inversível à direita para algum $y \in R$. Segue que $(1 - xy)R \neq R$, e então $(1 - xy)R$ é ideal à direita e próprio de R. De forma análoga ao que fizemos na Proposição 1.6, existe um ideal maximal à direita M de R tal que $(1 - xy)R \subseteq M$. Em particular, $1 - xy \in M$. Como $x \in J(R) \subseteq M$ temos que $xy \in M$ que implica $1 - xy + xy = 1 \in M$. Absurdo. Logo, $1 - xy$ é inversível à direita.

($\Leftarrow$) Suponha $x \notin J(R)$. Então $x \notin M$, para algum ideal maximal à direita M. Mas então:

$$\begin{aligned} M \subsetneq xR + M \subseteq R \Rightarrow xR + M = R \Rightarrow \exists y \in R,\ m \in M \text{ tal que } xy + m = 1 \\ \Rightarrow 1 - xy \in M \end{aligned}$$

Logo, $1 - xy$ não é inversível à direita. Absurdo. Logo, $x \in J(R)$.

(ii) Tomemos J ideal tal que para todo $y \in J, 1 - y$ é inversível. Seja $x \in J$. Para todo $r \in R$ temos $xr \in J$, ou seja, $1 - xr$ é inversível qualquer que seja $r \in R$. Portanto, $x \in J(R)$. Logo, $J \subseteq J(R)$.

■

Notações:

- $Nil(R)$ - indica a intersecção dos ideais primos nil semi-simples de R.
- $Ng(R)$ - indica a intersecção dos ideais completamente primos de R.
- $s(R)$ - indica a intersecção dos ideais fortemente primos de R.
- $z(R)$ - indica a intersecção dos ideais primos não singulares de R.
- $G(R)$ - indica a intersecção dos ideais maximais de R.

Como cada um dos conjuntos acima é uma intersecção de ideais de R, concluímos que todos estes conjuntos são ideais de R. Vamos provar que são radicais de R.

Proposição 3.6 *: Seja R um anel. Então:*

(a) $Nil\left(\dfrac{R}{Nil(R)}\right) = \{\overline{0}\}$.

(b) $Ng\left(\dfrac{R}{Ng(R)}\right) = \{\overline{0}\}$.

(c) $s\left(\dfrac{R}{s(R)}\right) = \{\overline{0}\}$.

(d) $z\left(\dfrac{R}{z(R)}\right) = \{\overline{0}\}$.

(e) $G\left(\dfrac{R}{G(R)}\right) = \{\overline{0}\}$.

Demonstração: (a) Seja $\overline{x} = x + Nil(R) \in Nil\left(\dfrac{R}{Nil(R)}\right)$. Então $\overline{x}$ está em todo ideal primo nil semi-simples de $\dfrac{R}{Nil(R)}$.

Seja P um ideal primo nil semi-simples de R. Por definição temos $Nil(R) \subseteq P$, e podemos montar o anel quociente $\dfrac{P}{Nil(R)}$. Temos que $\dfrac{P}{Nil(R)}$ é ideal do anel $\dfrac{R}{Nil(R)}$.

Agora vamos mostrar que $\dfrac{P}{Nil(R)}$ é ideal primo de $\dfrac{R}{Nil(R)}$.

Sejam $\dfrac{A}{Nil(R)}$ e $\dfrac{B}{Nil(R)}$ ideais de $\dfrac{R}{Nil(R)}$ tais que $\dfrac{A}{Nil(R)}.\dfrac{B}{Nil(R)} \subseteq \dfrac{P}{Nil(R)}$. Segue que $AB \subseteq P$ e, como P é primo, temos $A \subseteq P$ ou $B \subseteq P$. Portanto $\dfrac{A}{Nil(R)}$ ou $\dfrac{B}{Nil(R)}$ deve estar contido em $\dfrac{P}{Nil(R)}$ e, daí, $\dfrac{P}{Nil(R)}$ é ideal primo.

O próximo passo é provar que $\dfrac{P}{Nil(R)}$ é ideal primo nil semi-simples de $\dfrac{R}{Nil(R)}$. Por definição, basta provar que $\dfrac{\frac{R}{Nil(R)}}{\frac{P}{Nil(R)}}$ não possui nil ideais não nulos.

Como P é ideal primo nil semi-simples de R vem que $\dfrac{R}{P}$ não tem nil ideais não nulos. Agora, o isomorfismo

$$\frac{\frac{R}{Nil(R)}}{\frac{P}{Nil(R)}} \simeq \frac{R}{P}$$

garante que $\dfrac{\frac{R}{Nil(R)}}{\frac{P}{Nil(R)}}$ não tem nil ideais não nulos.

Concluímos que $\dfrac{P}{Nil(R)}$ é ideal primo nil semi-simples de $\dfrac{R}{Nil(R)}$.

Pela escolha de $\overline{x}$ no início da demonstração, vem que $\overline{x} \in \dfrac{P}{Nil(R)}$. Logo $x \in P$. Como P é um ideal primo nil semi-simples arbitrário, concluímos que $x \in Nil(R)$. Portanto $\overline{x} = x + Nil(R) = \overline{0}$.

(b) Seja $\overline{x} = x + Ng(R) \in Ng\left(\dfrac{R}{Ng(R)}\right)$. Então $\overline{x}$ está em todo ideal completamente primo de $\dfrac{R}{Ng(R)}$.

Seja P um ideal completamente primo de R. Por definição temos, $Ng(R) \subseteq P$, e daí $\dfrac{P}{Ng(R)}$ é ideal $\dfrac{R}{Ng(R)}$. Vamos ver que este ideal é completamente primo.

Sejam $\overline{r}, \overline{s} \in \dfrac{R}{Ng(R)}$ tais que $\overline{r}.\overline{s} \in \dfrac{P}{Ng(R)}$. Segue que $rs \in P$ e, como P é ideal completamente primo, vem que $r \in P$ ou $s \in P$. Então $\overline{r}$ ou $\overline{s}$ está em $\dfrac{P}{Ng(R)}$ e, daí, $\dfrac{P}{Ng(R)}$ é ideal completamente primo de $\dfrac{R}{Ng(R)}$.

Pela escolha de $\overline{x}$, vem que $\overline{x} = x + Ng(R) \in \dfrac{P}{Ng(R)}$. Logo, $x \in P$ e, então, $x \in Ng(R)$. Portanto $\overline{x} = \overline{0}$.

(c) Seja $\overline{x} = x + s(R) \in s\left(\dfrac{R}{s(R)}\right)$. Então $\overline{x}$ está em todo ideal fortemente primo de $\dfrac{R}{s(R)}$.

Seja P um ideal fortemente primo de R. Por definição, temos $s(R) \subseteq P$, e daí $\dfrac{P}{s(R)}$ é ideal $\dfrac{R}{s(R)}$. Vamos ver que este ideal é fortemente primo.

Como P é ideal fortemente primo de R, vem que $\dfrac{R}{P}$ é anel fortemente primo. Agora, o isomorfismo

$$\frac{\dfrac{R}{s(R)}}{\dfrac{P}{s(R)}} \simeq \frac{R}{P},$$

garante que $\dfrac{P}{s(R)}$ é ideal fortemente primo de $\dfrac{R}{s(R)}$. Pela escolha de $\overline{x}$ temos que $\overline{x} = x + s(R) \in \dfrac{P}{s(R)}$. Então $x \in P$, e daí $x \in s(R)$. Logo $\overline{x} = x + s(R) = \overline{0}$.

(d) Seja $\overline{x} = x + z(R) \in z\left(\dfrac{R}{z(R)}\right)$. Então $\overline{x}$ está em todo ideal primo não singular de $\dfrac{R}{z(R)}$.

Seja P um ideal primo não singular de R. Por definição temos $z(R) \subseteq P$, e daí $\dfrac{P}{z(R)}$ é ideal $\dfrac{R}{z(R)}$. Além disso, de forma análoga a feita no caso (a), pode-se provar que $\dfrac{P}{z(R)}$ é ideal primo de $\dfrac{R}{z(R)}$.

Agora vamos mostrar que $\dfrac{P}{z(R)}$ é ideal não singular de $\dfrac{R}{z(R)}$. Por definição, basta verificar que $\dfrac{\frac{R}{z(R)}}{\frac{P}{z(R)}}$ é anel não singular.

Como P é ideal primo não singular temos que $\dfrac{R}{P}$ é anel não singular e, via isomorfismo $\dfrac{\frac{R}{z(R)}}{\frac{P}{z(R)}} \simeq \dfrac{R}{P}$ obtemos que $\dfrac{P}{z(R)}$ é ideal primo não singular de $\dfrac{R}{z(R)}$.

Segue que $\overline{x} = x + z(R) \in \dfrac{P}{z(R)}$. Então $x \in P$, e daí $x \in z(R)$. Portanto $\overline{x} = \overline{0}$.

(e) Seja $\overline{x} = x + G(R) \in G\left(\dfrac{R}{G(R)}\right)$. Então $\overline{x}$ está em todo ideal maximal de $\dfrac{R}{G(R)}$.

Seja M um ideal maximal de R. Por definição, temos $G(R) \subseteq M$ e então $\dfrac{M}{G(R)}$ é ideal $\dfrac{R}{G(R)}$. Vamos provar que este ideal é maximal.

Se $\dfrac{I}{G(R)}$ é ideal de $\dfrac{R}{G(R)}$ tal que $\dfrac{M}{G(R)} \subseteq \dfrac{I}{G(R)} \subseteq \dfrac{R}{G(R)}$, então I é ideal de R tal que $M \subseteq I \subseteq R$. A maximalidade de M garante que $I = M$ ou $I = R$. Então $\dfrac{I}{G(R)} = \dfrac{M}{G(R)}$ ou $\dfrac{I}{G(R)} = \dfrac{R}{G(R)}$. Segue que $\dfrac{M}{G(R)}$ é ideal maximal de $\dfrac{R}{G(R)}$, e daí, $\overline{x} = x + G(R) \in \dfrac{M}{G(R)}$. Segue que $x \in M$. Então $x \in G(R)$ e $\overline{x} = \overline{0}$.

■

Definição 3.6 : *O radical $Nil(R)$ é chamado nil radical superior de R.*

Definição 3.7 : *O radical $Ng(R)$ é chamado nil radical generalizado de R.*

Definição 3.8 : *O radical $s(R)$ é chamado radical fortemente primo de R.*

Definição 3.9 : *O radical $z(R)$ é chamado radical singular de R.*

Definição 3.10 : *O radical $G(R)$ é chamado radical de Brown-McCoy de R.*

As relações de inclusão entre classes de ideais primos:

$$
\begin{array}{ccccccc}
\mathcal{C}(R) & \subseteq & \mathcal{S}(R) & \subseteq & \mathcal{Z}(R) & \subseteq & P(R) \\
 & & \rotatebox[origin=c]{90}{$\subseteq$} & & & & \rotatebox[origin=c]{90}{$\subseteq$} \\
 & & \mathcal{M}(R) & \subseteq & p(R) & \subseteq & \mathcal{N}(R)
\end{array}
$$

levam às seguintes relações de inclusão entre os radicais

$$
\begin{array}{ccccccc}
\beta(R) & \subseteq & z(R) & \subseteq & s(R) & \subseteq & Ng(R) \\
\rotatebox[origin=c]{-90}{$\subseteq$} & & & & \rotatebox[origin=c]{-90}{$\subseteq$} & & \\
Nil(R) & \subseteq & J(R) & \subseteq & G(R) & &
\end{array}
$$

Referências

[1] GONÇALVES, A. - *Introdução à Álgebra*. Rio de Janeiro, IMPA, 1979.

[2] DOMINGUES, H. H.; IEZZI, G. - *Álgebra Moderna*. Atual Editora, São Paulo, 1996.

[3] FERRERO, M. - *Ideais Primos em Extensões de Anéis*. Atas da XIII Escola de Álgebra - UNICAMP, 1994.

[4] LANG, S. - *Estruturas Algébricas*. Nova Iorque, Universidade de Columbia, 1972.

[5] GARCIA, A.; LEQUAIN, Y. - *Elementos de Álgebra*. Rio de Janeiro, IMPA, 1988.

[6] HALMOS, P. - *Teoria Ingênua dos Conjuntos*. Ed. Ciência Moderna, Rio de Janeiro, 2001.

[7] MCCOY, N. H. - *The theory of Rings*. Mac Millan Co., New York, 1964.

[8] REINER, I. - *Maximal Orders*. Academic Press, London, 1975.