

1) Se N é um inteiro composto que (N) não é um ideal primo \mathbb{Z} .

Números compostos: são aqueles que resultam da multiplicação de números primos.

Ex: $6 = 2 \cdot 3$, $9 = 3^2$, etc

Tomemos N sem inteiros compostos, ou seja, para $j=1, \dots, N$:

$$N_1 = a \cdot b$$

$$N_2 = a \cdot b \cdot c$$

$$\vdots$$

$$N_N = a \cdot b \cdot \dots \cdot c$$

Tomemos que (N) , ideal de inteiros compostos, definimos ideal primo.

Ideal primo: Sejam A um anel, seja p um ideal primo de A . Dizemos que " p " é um ideal primo de A se "para qualquer $a, b \in A$ tais que $ab \in p$ tem-se que $a \in p$ e $b \in p$ ".

Tomamos N um inteiro composto, e um certo " p " primo, sendo $N = a \cdot b$. Logo, se:

$$p \mid N \rightarrow p \mid ab \text{ e } p \mid a \text{ ou } p \mid b$$

Mas N não é primo, então (N) é um ideal gerador de N para inteiros não primos, logo (N) não gera um ideal primo em \mathbb{Z} .

Prove: (n) ideal primo de $\mathbb{Z} \hookrightarrow n$ é primo
se $n \neq 0$

Definição: Ideal primo (n) :

$$ab \in (n) \rightarrow a \in (n) \text{ ou } b \in (n)$$

Def(1): n é um inteiro primo se $n \neq 0, \pm 1$ e somente
não divisões $\pm n, \pm 1$.

Def(2): n é primo se $n \neq 0, \pm 1$ somente divisões
de n são $\pm 1, \pm n$.

$$n/a \rightarrow n/a \text{ ou } n/b$$

i) Ideal primo (n) de $\mathbb{Z} \rightarrow n$ é primo ou zero

Agora vamos considerar o caso onde $|n| \neq |0|$,
isto é, $n \neq 0$. Usando a definição de ideais
primos:

$$\begin{aligned} ab \in (n) &\rightarrow a \in (n) \text{ ou } b \in (n), \text{ se um elemento} \\ x \in (n) &\leftarrow x = q \cdot n \leftarrow n/x \end{aligned}$$
$$n/a \rightarrow n/a \text{ ou } n/b$$

Então, n é primo e diferente de zero.

ii) No caso que $|n| = |0|$ claramente $n=0$, dando
que não existem divisões diferentes de zero em
 \mathbb{Z} . Assim: n é primo ou zero $\rightarrow (n)$ é um
ideal primo de \mathbb{Z} .

Considere o caso onde n é primo, e $n \neq 0, \pm 1$.

$$n/a \rightarrow n/a \text{ ou } n/b$$

$$ab \in (n) \rightarrow a \in (n) \text{ ou } b \in (n)$$

No caso $N=0$, desde que \mathbb{Z} não tem divisores de zero:

$$ab=0 \rightarrow a=0 \text{ ou } b=0$$

Então (0) é um ideal primo.

2) Se R é um anel comutativo finito com identidade, provar que cada ideal primo em R é maximal.

Corolário: em um anel comutativo R com identidade, cada ideal maximal é primo.

Teorema 6.5: Temos M sendo um ideal em anel comutativo R com identidade. Então M é um ideal maximal, se e somente, se o anel quociente R/M é um domínio.

Temos R sendo um anel finito com unidade. Dizemos, que I sendo um ideal primo em R .

i) R/I é um domínio de integridade:

$$\langle 1_{R/I} \rangle = \infty$$

ii) R/I é um conjunto (dado que o domínio de integridade é um conjunto).

iii) I é um ideal maximal em R

Isso é, qualquer ideal é ideal maximal em um anel finito comutativo com unidade.

Desta forma temos que é verdadeiro, assim se um anel não tem identidade, o quociente por primos tem identidade. E cada anel finito diferente de zero tem divisões de zero tem uma identidade multiplicativa, assim o quociente poderia de fato ser um domínio finito com identidade.

Tomamos um anel comutativo com identidade R de cardinalidade m .

Temos que qualquer $I \subset R$ deve possuir cardinalidade i . Então:

$$I \subset R \rightarrow i \leq m$$

Temos que um ideal primo quando possui identidade, ou seja, possui 1 como elemento do conjunto. E é formado por "p" primo.

Como $i \leq m$, então $I \subset M$ ou $I = M$, mas é $I \subset M$ e $i < m$ por definição.

Temos que I é ideal com unidade, e como I é primo (ou seja gerado por primos) pelo corolário, em um anel comutativo R com identidade, cada maximal é primo.

Como o I (ideal) é primo, temos que é maximal.

3) a) Prove que um íntimo diferente de zero p
é primo, se e somente se, o ideal (p) é
maximal em \mathbb{Z} .

Definição: Sejam A um anel e $I \triangleleft A$.
Dizemos que I é ideal primo de A ,
se, para todo $a, b \in A$,

$$ab \in I \rightarrow a \in I \text{ ou } b \in I$$
$$I \subset A \text{ e } ab \in I \rightarrow a \in I$$

Definição: Sejam A um anel e $I \triangleleft A$, com $I \neq A$.
Dizemos que I é ideal maximal de A se
para qualquer $J \triangleleft A$ tal que $I \subset J$,
conclui-se que $J = I$ ou $J = A$.

A última definição significa que um ideal
é maximal se acima dele não há outros ideais
não triviais.

Ex: Considere $3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\} \triangleleft \mathbb{Z}$.

$3\mathbb{Z}$ é ideal primo de \mathbb{Z}

Então: $ab \in 3\mathbb{Z} \rightarrow \begin{cases} a \in 3\mathbb{Z} \\ b \in 3\mathbb{Z} \end{cases}$

Pois quaisquer $a, b \in \mathbb{Z}$, temos: $ab \in 3\mathbb{Z} \rightarrow$
 $ab = 3x (x \in \mathbb{Z}) \rightarrow 3 | ab \rightarrow 3 \text{ é primo}$

$\rightarrow 3 | a$ ou $3 | b \rightarrow a = 3y$ e $b = 3z$,
para $y, z \in \mathbb{Z} \rightarrow a \in 3\mathbb{Z}$ ou $b \in 3\mathbb{Z}$

• $3\mathbb{Z}$ é maximal em \mathbb{Z} . ($3\mathbb{Z} \subset J$ ou $3\mathbb{Z} \subset \mathbb{Z}$)

Pois, seja J um ideal de \mathbb{Z} tal que:

$$3\mathbb{Z} \subset J \subset \mathbb{Z}$$

Como \mathbb{Z} é anel principal, existe um inteiro
 n tal que $J = n\mathbb{Z}$.

$N\mathbb{Z}$ = gerado por N ou $\langle N \rangle$

Há dois casos:

i) Se $3 \mid N$, então $N = 3x$ ($x \in \mathbb{Z}$)

Então, para qualquer $ny \in J = N\mathbb{Z}$, tem-se $ny = 3Ny \in 3\mathbb{Z}$. Logo, $J \subset 3\mathbb{Z}$. E portanto $3\mathbb{Z} = J$

ii) Se $3 \nmid N$, então $\text{mdc}(3, N) = 1$

Pelo Teorema de Bezout, existem $g, d \in \mathbb{Z}$ tais que $3g + Nd = 1$

Para qualquer $n \in \mathbb{Z}$, então: $n = n \cdot 1 = n \cdot (3g + Nd)$
 $= 3ng + nNd \in J$.

Se $3g \in J$ e $nd \in J$, então: $3ng + nNd \in J$

Portanto, $2\mathbb{Z}J \subset \mathbb{Z} = J$

Tomamos p primo, dado $p = \{1, 2, 3, \dots\}$

Se $p=1 \rightarrow I_1 = \{1, 2, 3, 4, \dots\} = \mathbb{Z}^* \subset \mathbb{Z}$
Temos que I_1 é maximal.

Se $p=2 \rightarrow I_2 = \{2, 4, 6, 8, \dots\} = \mathbb{Z}_{(2)}^* \subset \mathbb{Z}$
Temos que I_2 é maximal

Se $p=N$ e N primo, temos que $\{N, 2N, 3N, \dots\} = N\mathbb{Z}^*$

$N\mathbb{Z}^* \subset \mathbb{Z}$, logo I_N é maximal

Põa $p = N+1$, temos que:

$$\{N, 2N, 3N, \dots\} + \{1, 2, 3, \dots\} = \{N+1, 2N+1, \dots\}$$

Logo: $(N+1)\mathbb{Z}^*$ é maximal

Portanto dado p inteiro diferente de zero,
temos que \mathbb{Z}_p é maximal em \mathbb{Z} .

b) Temos F sendo um corpo e $p(x) \in F[x]$.
Prove que $p(x)$ é irreduzível se e somente
se o ideal $(p(x))$ é maximal em $F[x]$.

Se $(p(x))$ não é maximal, então existe um
ideal I contendo $(p(x))$. Assim, temos mostrar
que:

$$I = F[x] \text{ ou } I = (p(x)).$$

Desde que $F[x]$ é um domínio ideal principal,
sabe-se que $I = (f(x))$ para algum polinômio $f(x)$.

Agora a contenção dos ideais $(p(x)) \subseteq (f(x))$ implica que $f(x)$ divide $p(x)$. Mas $p(x)$ é irreduzível, então isto somente é possível se $f(x)$ é um escalar múltiplo de $p(x)$, ou se $f(x)$ é constante.

Estes casos correspondentes implicam:

$$(f(x)) = (p(x)), \text{ ou } (f(x)) = F[x].$$

4) Temos R sendo um anel comutativo com identidade. Prove que R é um domínio de integridade se e somente se (0_R) é um primo ideal.

Suponhamos que R é um domínio de integridade, então R tem pelo menos 2 elementos (desde que $1 \neq 0$) e assim o ideal (0_R) não é anel R por ele mesmo.

Além disso, supomos que $a, b \in R$ e que $a \in (0_R)$ e que $b \notin (0_R)$. Assim $a \neq 0$ e $b \neq 0$. Desde que R é um domínio integral, segue-se que $ab \neq 0$.

Assim $ab \notin (0_R)$. Temos que mostrar que se $a \notin (0_R)$ e $b \notin (0_R)$, então $ab \notin (0_R)$. Desde que (0_R) não está em R . Seque-se que (0_R) é de fato um ideal primo de R .

Domínio de integralidade: é um anel comutativo com identidade sem divisores de zero.
 $\exists: ab=0 \rightarrow a=0 \text{ ou } b=0$ (não tem divisores de zero.)

Por outro lado, supomos que R é um anel comutativo com unidade $1 \neq 0$ e que (0_R) é um ideal primo de R .

Para mostrar que R é um domínio integral, devemos provar que para $a, b \in R$, se $a \neq 0$ e $b \neq 0$, então $ab \neq 0$. Para provar, isto assumimos que a e b são elementos diferentes de zero em R .

Então $a \notin (0_R)$ e $b \notin (0_R)$, desde que (0_R) é um ideal primo em R , logo $ab \notin (0_R)$. Assim $ab \neq 0$.

Com isso provamos que R é um domínio integral.

Teorema: Todo ideal maximal é primo.

Demonastração: Seja $I \triangleleft A$ ideal maximal qualquer. Mostremos que I é primo.
Sejam $a, b \in A$ tais que $ab \in I$. Suponha que $a \notin I$, mostremos que $b \in I$.

Seja $f = \langle a \rangle + I$. Assim:

- O conjunto f é um ideal de A

A soma de dois ideais é um ideal: $\langle a \rangle + I = f$.

Assim $I \subset f$, pois, se $y \in I$, então $y = a \cdot 0 + y \in f$ e $a \in f$, pois, $a \cdot 1 + 0 \in f$.

Como $a \notin I$, então $I \subset f \subset A$, e como f é maximal. Concluímos que $f = A$.

Isto significa que $1 \in A$ pode ser escrito como $1 = ac + x$, com $c \in I$ e $x \in I$.

Multiplicando esta expressão por b , temos

$$b = b(ac + x) = \underbrace{abc}_{\in I} + \underbrace{bx}_{\in I} \in I$$

Como um elemento pertence ao ideal, o produto também pertence ao ideal.

Logo, $b \in I$. Então I é um ideal primo.

Exemplo: O ideal $\langle x^2 + 1 \rangle$ é maximal em $\mathbb{Q}[x]$.

De fato, suponha que exista um ideal $J \supset \langle x^2 + 1 \rangle$ tal que $\langle x^2 + 1 \rangle \subset J \subset \mathbb{Q}[x]$.

Suponha que $\langle x^2 + 1 \rangle \subset J$. Assim, existe $p \in J$ tal que $p \notin \langle x^2 + 1 \rangle$.

Pela divisão de polinômios, existem $q, r \in \mathbb{Q}[x]$ tais que:

$$p = (x^2 + 1)q + r, \quad \text{grau}(r) < 2, \quad r \neq 0$$

Então $r = ax + b$, com $a, b \in \mathbb{Q}$ não simultaneamente nulos. Daí, $ax + b = p - (x^2 + 1)q \in J$. Assim,

$$a^2 + b^2 = a^2x^2 + a^2 - (a^2x^2 - b^2) = a^2(x^2 + 1) - (ax - b).$$
$$(ax + b) \in J.$$

Como $c = a^2 + b^2 \in J$, então $1 = c \cdot \frac{1}{c} \in J$.

Todo ideal com unidade é um anel, ou seja, $1 \in I$ então I é um anel.

Portanto, $\langle x^2 + 1 \rangle$ é maximal.

Exemplo: O ideal $\langle x^2 + 1 \rangle$ é primo.

De fato, como $\langle x^2 + 1 \rangle$ é maximal, segue do teorema 1 que $\langle x^2 + 1 \rangle$ é um ideal primo em $\mathbb{Q}[x]$.

O exemplo a seguir mostra que não vale a recíproca do Teorema 1, ou seja, que nem todo ideal primo é maximal.

Se $A = \mathbb{Z}$ vale a recíproca, mas para um A qual não.

Exemplo: Sejam $A = \mathbb{Z}[x]$ e $I = \langle x \rangle$

O ideal I é primo, pois, para qualquer $p, q \in \mathbb{Z}[x]$,

$$pq \in \langle x \rangle \rightarrow pq = a_0 + a_1 x^2 + \dots + a_n x^{n+1} \rightarrow p(0)q(0) = 0 \rightarrow p(0) = 0 \text{ ou } q(0) = 0 \rightarrow$$

$$p = b_0 x + b_1 x^2 + \dots + b_m x^m \text{ ou } q = c_0 x + c_1 x^2 + \dots + c_k x^k$$

Portanto, $\mathbb{Z}\langle x \rangle$ não é maximal. Assim $p \in \langle x \rangle$ ou $q \in \langle x \rangle$. Portanto I é um ideal primo.

Para $p(x)$ ou $q(x)$ em $p(0)$ ou $q(0)$ ser igual a zero, se $p(x)$ e $q(x)$ não tiver termo com coeficiente constante.

Ex: $\langle x_1, 2 \rangle = \{ax + 2b \mid a, b \in \mathbb{Z}[x]\}$

$$\begin{aligned} \langle x \rangle &\subseteq \langle x_1, 2 \rangle \quad (\langle x_1, 2 \rangle \in \mathbb{Z}\langle x \rangle) \\ \langle 2 \rangle &\subset \langle x_1, 2 \rangle \end{aligned}$$

Portanto existem ideais primos que não são maximais.

Exemplo: O ideal $I = \langle x^2 + \bar{1} \rangle$ não é primo em $\mathbb{Z}_2[x]$.

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\} \rightarrow \mathbb{Z}_2[x] = \{a_0 + a_1x + \dots + a_Nx^N\}$
com $a_i \in \{\bar{0}, \bar{1}\}$ e $i=0, \dots, N$

$$(x+\bar{1})^2 = x^2 + \bar{2}x + \bar{1} = x^2 + \bar{0}x + \bar{1} = x^2 + \bar{1}$$

Assim: $x^2 + \bar{1} = (x+\bar{1})(x+\bar{1})$, mas o polinômio $p = x+\bar{1} \notin \langle x^2 + \bar{1} \rangle$.

Pois se $(x+\bar{1}) \subseteq (x^2 + \bar{1})$, onde $p(x) \in \mathbb{Z}_2[x]$
 $\text{grau}=1 \neq \text{grau}=2$
Logo é impossível.

Assim $ab \in \langle x^2 + \bar{1} \rangle$, agora se $a = (x+\bar{1})$ e $b = (x+\bar{1})$ mas $a, b \notin \langle x^2 + \bar{1} \rangle$

Portanto $\langle x^2 + \bar{1} \rangle$ não é um ideal primo.

Teorema: Se A é um anel de integridade principal, então todo ideal primo não zero de A é maximal.

anel de integridade principal:

Anel de integridade: é um anel comutativo com identidade sem divisores de zero. " $ab=0 \rightarrow a=0$ ou $b=0$ ".

Um anel de integridade R com elemento unidade é um anel principal se todo ideal A em R é da forma $A = aR$ para algum $a \in R$.

Demô: De fato, seja $I \neq A$ ideal primo tal que

Como A é principal, então $I = \langle \alpha \rangle = \alpha I$ e $\alpha \neq 0$.

Alja $f \in A$ tal que: $I \subset f \subset A^*$, assim:

$I \subseteq f \subseteq A$ Como A é principal, $f = \langle \beta \rangle$.
 \downarrow \downarrow Como $\langle \alpha \rangle \subset \langle \beta \rangle$, então
 $\langle \alpha \rangle \subset \langle \beta \rangle$ existe $a \in A$ tal que $\alpha = \beta a$.

Temos que $\alpha \in \langle \alpha \rangle \rightarrow \alpha \in \langle \beta \rangle$ e como I é primo e $\alpha \in I$, então $\beta \in I$ ou $a \in I$.

Caso 1: Se $\beta \in I$, então $f = \langle \beta \rangle \subset I$, logo de I que $I = f$.

Caso 2: Se $a \in I$, então existe $b \in A$ tal que $a = \beta b$.
Então:

$$\alpha = \beta a = \beta \beta b \rightarrow \alpha(1 - \beta b) = 0.$$

Algarismo da integridade (comutativo) de A que $\alpha = 0$ ou $1 - \beta b = 0$. Com $\alpha \neq 0$, então $\beta b = 1$.

Dado qualquer $x \in A$, então $x = x \cdot 1 = x \beta b \in \langle \beta \rangle = f$.

Portanto, A é maximal.

Teorema: Sejam A um anel comutativo e I s.t.
então A/I é anel de integridade se, e somente se, I é ideal primo.

Demo: i) Suponha que A/I é anel de integridade.
Então: $ab \in I \rightarrow I = ab + I = (a+I)(b+I)$

$$x \in I \text{ e } x \neq 0 \in f \rightarrow x + I = 0 + x = I$$

$$x + I = y + I \hookrightarrow x - y = I$$

Como A/\mathbb{I} é de integridade, então $a+\mathbb{I}=\mathbb{I}$
ou $b+\mathbb{I}=\mathbb{I}$.

$$(a+\mathbb{I})(b+\mathbb{I}) = \mathbb{I} \text{ (neutro)} \rightarrow \begin{cases} a+\mathbb{I}=\mathbb{I} \\ b+\mathbb{I}=\mathbb{I} \end{cases}$$

ii) Suponha que \mathbb{I} é um ideal primo:

Se $(a+\mathbb{I})(b+\mathbb{I}) = \mathbb{I}$, então $ab+\mathbb{I}=\mathbb{I}$. Daí, $ab \in \mathbb{I}$.
Como \mathbb{I} é ideal primo, então $a \in \mathbb{I}$ ou $b \in \mathbb{I}$.
Portanto, $a+\mathbb{I}=\mathbb{I}$ ou $b+\mathbb{I}=\mathbb{I}$.

Logo, como A/\mathbb{I} é comutativo, então
 A/\mathbb{I} é anel de integridade.

Teorema: Sejam A um anel comutativo e
 $\mathbb{I} \triangleleft A$. Então A/\mathbb{I} é corpo se, e somente se, \mathbb{I} é
ideal maximal.

Ideal principal: ideal gerado por um único elemento.

Anel principal: anel gerado por ideais principais.
Ex: \mathbb{Z}

5) Liste todos os ideais maximais em \mathbb{Z}_6 , faça o
mesmo em \mathbb{Z}_{12} .

ii) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ em um anel \mathbb{Z} .

Ideal: $x \in \mathbb{Z}_6$ e $a \in \mathbb{Z} \rightarrow x.a \in \mathbb{Z}_6 \wedge a.x \in \mathbb{Z}_6$.
Como \mathbb{Z} é comutativo, podemos fazer uma
multiplicação única.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$\{0\} \subset \mathbb{Z}_6 \rightarrow 0 \cdot x = x \cdot 0 \in \mathbb{Z}_6$. $\{0\}$ é maximal

Agora temosmos I sendo um ideal de \mathbb{Z}_6 . Se I contém uma unidade, $a \in I$ então:

$a \cdot a^{-1} = 1 \in I$, $[1] \in I$ sendo $[1]$ um gerador de \mathbb{Z}_6 . Assim, para qualquer $[b] \in \mathbb{Z}_6$ temos que $[b] = [b][1] \in I$. Portanto $I = \mathbb{Z}_6$.

Se $I \neq \mathbb{Z}_6$ então $I \cap \{[0], [2], [3], [4]\}$ são os conjuntos sem unidade de \mathbb{Z}_6 . Isto porque $\{[1], [5]\}$ têm unidade.

Observe que I deve ser um subconjunto estrito desde que se $[2], [3] \in I$ então:

$$[3] - [2] = [1] \in I$$

Isto implica que $I = \mathbb{Z}_6$.

Sabemos que $[0] \in I$, podemos verificar que os seguintes subconjuntos são ideais principais:

$$\{[0]\}$$

$\{[0], [2], [4]\} = \{[2]\} = \{[4]\}$ Além disso, os subconjuntos: $\{[0], [2]\} \subset \{[0], [2], [4]\}$, $\{[0], [2], [4]\} \subset \{[0], [2], [3]\}$, $\{[0], [2], [3]\} \subset \{[0], [2], [3], [4]\}$ não são ideais.

Portanto, \mathbb{Z}_6 tem um total de 2 ideais não-triviais:

$$\{[0], [3]\} = \{[3]\}$$

$\{[0], [2], [4]\} \subset \{[0], [3]\}$ Eles são ambos maximais.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \quad (\mathbb{Z}_6, +_6, \cdot_6)$$

$$1/6 \Rightarrow \langle 1 \rangle = \mathbb{Z}_6$$

$$2/6 \Rightarrow \langle 2 \rangle = \{0, 2, 4\}$$

$$3/6 \Rightarrow \langle 3 \rangle = \{0, 3\}$$

$$4/6 \Rightarrow \langle 4 \rangle = \{0, 2\}$$

Como $\langle 4 \rangle \subset \langle 2 \rangle$ e $\langle 3 \rangle \not\subset \langle 2 \rangle$ temos
2 ideais maximais.

$$\text{iii) } \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

$$1/\mathbb{Z}_{12} = \langle 1 \rangle = \mathbb{Z}_{12}$$

$$\langle 3 \rangle = \langle 9 \rangle = \mathbb{Z}_1$$

$$\langle 6 \rangle \subset \mathbb{Z}_1$$

$$2/\mathbb{Z}_{12} = \langle 2 \rangle = \{0, 2, 4, 8, 10\}$$

$$\langle 6 \rangle \subset \langle 2 \rangle$$

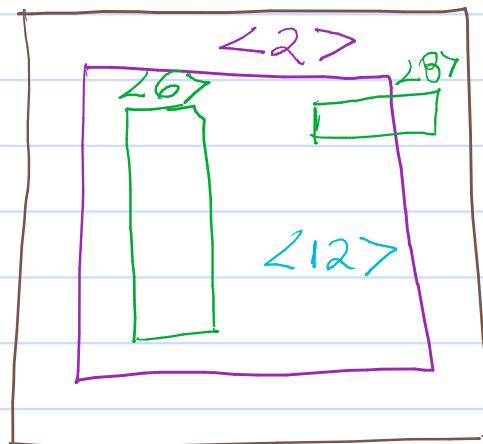
$$3/\mathbb{Z}_{12} = \langle 3 \rangle = \{0, 3, 6, 9\}$$

$$\langle 2 \rangle \subset \langle 6 \rangle$$

$$\langle 12 \rangle \subset \langle 6 \rangle$$

$$\langle 10 \rangle$$

$$4/\mathbb{Z}_{12} = \langle 4 \rangle = \{0, 4, 8\}$$



$$5/\mathbb{Z}_{12} = \langle 6 \rangle = \{0, 6\}$$

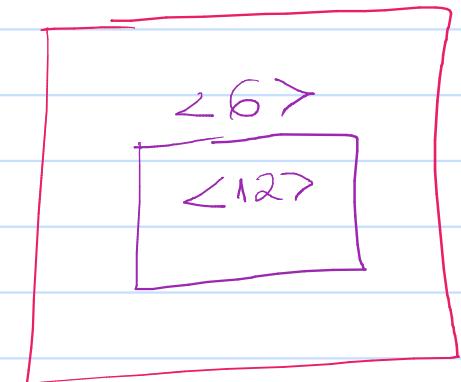
$$6/\mathbb{Z}_{12} = \langle 8 \rangle = \{0, 8, 4\}$$

$$7/\mathbb{Z}_{12} = \langle 9 \rangle = \{0, 9, 6, 3\}$$

$$8/\mathbb{Z}_{12} = \langle 10 \rangle = \{0, 10, 8, 6, 4, 2\}$$

$$9/\mathbb{Z}_{12} = \langle 12 \rangle = \{0\}$$

$$\langle 9 \rangle = \langle 3 \rangle$$



Ideais Maximaais: $\langle 10 \rangle$, somente um.

6) Mostre que existe exatamente um ideal maximal em \mathbb{Z}_8 . Faça o mesmo para \mathbb{Z}_9 .

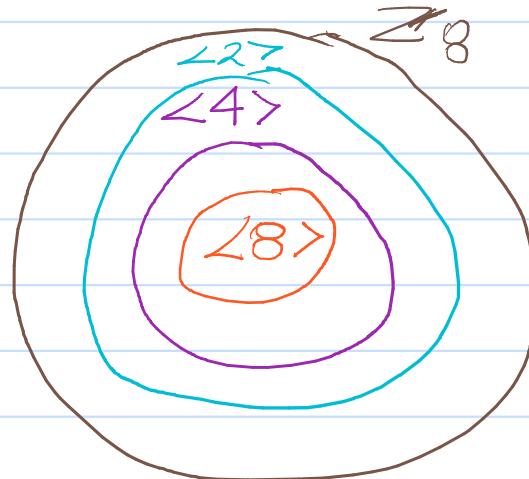
ii) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\} \quad (\mathbb{Z}_8, +_8, \cdot)$

$$1/\mathbb{Z}_8 \Rightarrow \langle 1 \rangle = \mathbb{Z}_8$$

$$2/\mathbb{Z}_8 \Rightarrow \langle 2 \rangle = \{0, 2, 4, 6\}$$

$$4/\mathbb{Z}_8 \Rightarrow \langle 4 \rangle = \{0, 4\}$$

$$8/\mathbb{Z}_8 \Rightarrow \langle 8 \rangle = \{0\}$$



$$\langle 8 \rangle \subsetneq \langle 4 \rangle \subsetneq \langle 2 \rangle \subsetneq \langle 1 \rangle = \mathbb{Z}_8$$

$\langle 2 \rangle$ é o único ideal maximal de \mathbb{Z}_8 .

iii) $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\langle 1 \rangle$ é o único ideal maximal de \mathbb{Z}_9 .

$$1/\mathbb{Z}_9 = \langle 1 \rangle = \mathbb{Z}_9$$

$$3/\mathbb{Z}_9 = \langle 3 \rangle = \{0, 3, 6\}$$

$$6/\mathbb{Z}_9 = \langle 6 \rangle = \{0, 6, 3\}$$

$$9/\mathbb{Z}_9 = \langle 9 \rangle = \{0\}$$

Pela definição o ideal maximal é o maior ideal ou igual a \mathbb{Z}_9 .

iii) Mostre que \mathbb{Z}_{10} e \mathbb{Z}_{15} têm mais de que um ideal maximal.

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \quad \langle 5 \rangle = \{0, 5\} = \langle 5 \rangle_{10}$$

$$1/\mathbb{Z}_{10} = \langle 1 \rangle = \mathbb{Z}_{10}$$

$$2/\mathbb{Z}_{10} = \langle 2 \rangle = \{0, 2, 4, 6, 8\}$$

$$4/\mathbb{Z}_{10} = \langle 4 \rangle = \{0, 4, 8, 2\}$$

$$\langle 10 \rangle = \{0, 6, 2, 8, 4\} = \langle 6 \rangle$$

$$\langle 8 \rangle = \{0, 8, 6, 4, 2\} = \langle 8 \rangle$$

$$\langle 10 \rangle = \{0\} = \langle 10 \rangle$$

$$\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \{0, 2, 4, 6, 8\}$$

$$\langle 10 \rangle \subset \langle 5 \rangle$$

Tem somente um ideal maximal, $\langle 1 \rangle = \mathbb{Z}_{15}$, pela definição é o conjunto com maior número de elementos.

$$iii) \mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

$$\langle 1 \rangle = \mathbb{Z}_{15}$$

$$\langle 3 \rangle = \langle 6 \rangle = \langle 9 \rangle \subset \langle 12 \rangle$$

$$\langle 1 \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12\}$$

$$\langle 1 \rangle = \langle 6 \rangle = \{0, 6, 12, 3, 9\}$$

$$\langle 1 \rangle = \langle 9 \rangle = \{0, 9, 3, 12, 6\}$$

$$\langle 1 \rangle = \langle 12 \rangle = \{0, 12, 9, 6, 3\}$$

$$\langle 1 \rangle = \langle 15 \rangle = \{0\}$$

Tem somente um ideal maximal $\langle 1 \rangle$ ou \mathbb{Z}_{15} .

Por definição de ideal maximal

$$\langle 1 \rangle = \langle 5 \rangle = \{0, 5, 10\}$$

7) Temos R sendo um anel comutativo com unidade. Prove que R é um conjunto se e somente se 10_R é um ideal maximal.

ii) Suponha que R é um conjunto e que f é um ideal de R sendo que $(0_R) \subset f \subset R$. Assumimos que $f \neq (0_R)$, então f contém um elemento diferente de zero a de R .

Desde que R é um conjunto, o elemento a é uma unidade em R .

$$aR = R$$

Desde que f é um ideal de R e $a \in f$,
 isto segue que $aR \subseteq f$. Assim $R \subseteq f$.
 Também temos que $f \subseteq R$, portanto, se
 $f \neq (0_R)$, temos que $f = R$. Consequentemente,
 (0_R) de fato é um ideal maximal de R .

Por outro lado, supomos que R é um anel
 comutativo com unidade $1 \neq 0$ e que
 (0_R) é um ideal maximal de R .

Supomos que $a \in R$ e que $a \neq 0$. Considere o
 ideal principal aR do anel R . O ideal
 aR contém o elemento diferente de a e
 assim $aR \neq (0_R)$.

Assim, aR é um ideal de R sendo que
 $(0_R) \subseteq aR \subseteq R$ e $aR \neq (0_R)$. Desde que

(0_R) é um ideal maximal de R , segue-se
 que $aR = R$. Em particular, temos $1 \in aR$.
 Assim, existe um elemento $b \in R$ sendo que
 $1 = ab$. Desde que R é um anel comutativo,
 temos também $ba = 1$. Assim, a é uma
 unidade em R . Temos que cada elemento
 de R é uma unidade em R . Sigue-se
 que R é um conjunto.

B) De um exemplo para mostrar que a infusão
 de 2 ideais primos não precisa ser
 um ideal primo.

Considera $I = 2\mathbb{Z}$ e $J = 3\mathbb{Z}$, I e J são ideais primos em \mathbb{Z} , mas $I \cap J = 6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$

Temos que $6\mathbb{Z}$ não é um ideal primo em \mathbb{Z} , isto porque:

$$2 \cdot 3 = 6 \in 6\mathbb{Z}, \text{ mas } 2 \notin 6\mathbb{Z} \text{ e } 3 \notin 6\mathbb{Z}$$

10) Temos p sendo um primo fixado e temos \mathcal{J} sendo o conjunto de polinômios em $\mathbb{Z}[x]$ cujos termos constantes são divisíveis por p . Prove que \mathcal{J} é um ideal maximal em $\mathbb{Z}[x]$.

Temos $p \in \mathbb{Z}$ e " p " primo, \mathcal{J} é um conjunto de polinômios em $\mathbb{Z}[x]$.

$p(x) \in \mathcal{J}$ com $p(x) = a_0 + a_1x + \dots + a_nx^n$ e $p \mid a_0$, então $p(0) \neq 0$.

Teorema: Todo ideal maximal é primo.

Tomamos " p " um número primo, \mathbb{Z}_p é um conjunto de números múltiplos de p .

① Definimos uma função $t: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p$ por $t(f(x)) = [a_0]$ onde $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Temos também $g(x) = b_mx^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0$. Então: $t(f(x) + g(x)) = [a_0 + b_0] = [a_0] + [b_0] = t(f(x)) + t(g(x))$ e $t(f(x) \cdot g(x)) = [a_0 \cdot b_0] = [a_0] \cdot [b_0] = t(f(x)) \cdot t(g(x))$. Então t é um isomorfismo.

$\forall [a] \in \mathbb{Z}_p$, então $f(x) = a \in \mathbb{Z}[x]$, e
 $t([a]) = [a]$, então t é subjetiva.

Além disso, o núcleo de t é $\{f(x) \in \mathbb{Z}[x] \mid t(f(x)) = 0\} = \{f(x) \in \mathbb{Z}[x] \mid p | f(x)\}$.

Pelo 1º Teorema do Isomorfismo, temos:

$\frac{\mathbb{Z}[x]}{f} \cong \mathbb{Z}_p$. Então \mathbb{Z}_p é um conjunto e
 f é um ideal maximal de $\mathbb{Z}[x]$.

U

II) Mostre que o ideal principal $(x-1)$ em $\mathbb{Z}[x]$ é primo mas não é maximal.

Definiremos $t: \mathbb{Z}[x] \rightarrow \mathbb{Z}$ por $t(f(x)) = f(1)$ onde

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Temos $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$. Então:

$$t(f(x) + g(x)) = f(1) + g(1) = t(f(x)) + t(g(x))$$

$$t(f(x) \cdot g(x)) = f(1) \cdot g(1) = t(f(x)) \cdot t(g(x))$$

Temos que t é um homomorfismo.

Se $a \in \mathbb{Z}$, então $f(x) = a \in \mathbb{Z}[x]$, e $t(f(x)) = f(1) = a$,
então t é sobrejetiva.

Além disso, o núcleo de t é $\{f(x) \in \mathbb{Z}[x] \mid t(f(x)) = 0\} = \{f(x) \in \mathbb{Z}[x] \mid x-1 \mid f(x)\} = \{f(x) \in \mathbb{Z}[x] \mid f(x) = 0\}$.

Prop 1º Teorema de Isomorfismo: $\frac{\mathbb{Z}[x]}{(x-1)} \cong \mathbb{Z}$

Como \mathbb{Z} é um domínio de integridade, temos que $(x-1)$ é um ideal principal, mas não é um ideal maximal.

2º Encontre um ideal em $\mathbb{Z} \times \mathbb{Z}$ que é primo mas não é maximal.

Definimos $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, por $f(z_1, z_2) = z_1$.

F é um homomorfismo sobrejetivo e o núcleo de f é $I = (0) \times \mathbb{Z}$. Então pelo 1º Teorema de Isomorfismo implica que:

$$\frac{\mathbb{Z} \times \mathbb{Z}}{(0) \times \mathbb{Z}} \cong \mathbb{Z}$$

Onde que \mathbb{Z} é um domínio integral, $(0) \times \mathbb{Z}$ é um ideal primo que não é maximal.

3º Seja p um primo inteiro, prove que M é um maximal ideal em $\mathbb{Z} \times \mathbb{Z}$, onde $M = \langle (pa, b) | a, b \in \mathbb{Z} \rangle$

Tomamos $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_p$ dada por $f(m, n) = \langle m \rangle_p$

Temos que f é um homomorfismo sobrejetivo e o núcleo de f é M . Isto porque se $m = 0 \Rightarrow f(m, n) = 0_p = 0$.

Com isso pelo 1º Teorema de Isomorfismo temos que $(\mathbb{Z} \times \mathbb{Z})/M$ é isomorfo a \mathbb{Z}_p e pelo

Teorema 6.16 Temos que M é maximal.

Teorema 6.13: 1º Teorema Isomorfismo

Temos $f: R \rightarrow S$ sendo um homomorfismo sobrejetivo de anéis com Núcleo K. Então o quociente anel R/K é isomórfico a S.

Teorema 6.16: Em anel comutativo R com identidade, cada ideal maximal é primo.

13) \overbrace{M} \overbrace{S} é um ideal em um anel R, então $I \times I$ é um ideal em $Z \times Z$ pelo exercício 8 da seção 6.1. Prove que $(R \times R)/(I \times I)$ é isomorfismo para $R/I \times R/I$.

(Dica: Mostre que a função $f: R \times R \rightarrow R/I \times R/I$ dada por $f(a, b) = (a+I, b+I)$ é um homomorfismo sobrejetivo de anéis com Núcleo $I \times I$.) \rightarrow Teorema 6.13.

Temos $I \subset R$ e I ideal de R. E $I \times I$ é um ideal em $Z \times Z$. Provar:

$\frac{R \times R}{I \times I} \rightarrow$ é isomorfo para $R/I \times R/I$.

Alguém a dica dada no exercício, considere a função: $f: R \times R \rightarrow R/I \times R/I$ dada por $f(a, b) = (a+I, b+I)$

Unde a, b $\in R$

Temos que, f é um homomorfismo assim:

$$\begin{aligned} \cdot f(a,b) + (c,d) &= f(a,b) + f(c,d) \\ \cdot f((a,b), (c,d)) &= f(a,b) \cdot f(c,d) \end{aligned}$$

Agora temos que mostrar que f é sobrejetiva, de fato, basta observar que dado:

$$(a+\mathbb{I}, b+\mathbb{I}) \in R/\mathbb{I} \times R/\mathbb{I} \rightarrow (a+\mathbb{I}, b+\mathbb{I}) = f(a,b)$$

Assim temos $\text{nuc}(f) = \mathbb{I} \times \mathbb{I}$. Supomos que $f(a,b) = 0$ então:

$$\begin{aligned} f(a,b) &= (a+\mathbb{I}, b+\mathbb{I}) = (0+\mathbb{I}, 0+\mathbb{I}) \rightarrow a+\mathbb{I} = 0+\mathbb{I} \text{ e} \\ b+\mathbb{I} &= 0+\mathbb{I} \end{aligned}$$

Logo, $a \in \mathbb{I}$ e $b \in \mathbb{I}$. Sabe-se que o $\text{nuc}(f)$ consiste dos elementos (a,b) com $a, b \in \mathbb{I}$, isto é, $\text{nuc}(f) = \mathbb{I} \times \mathbb{I}$.

Como f é sobrejetiva, temos pelo 1º Teorema de Isomorfismos que $\frac{R \times R}{\mathbb{I} \times \mathbb{I}}$ é isomórfico a $R/\mathbb{I} \times R/\mathbb{I}$.

g) Temos R sendo um domínio de integridade em que cada ideal é principal. Se (p) é um primo ideal diferente em R , prové que p tem esta propriedade: sempre que p fatores $|p = cd|$, então c ou d é uma unidade em R .

Temos (p) com um gerador primo de um ideal diferente cada primo p em R . Um ideal principal é gerado por um elemento.

Se $p = cd$ e c, d pertencem a R , temos que p é o produto de c e d .

Mas p é primo, então $p = cd$ é ^{impossível}, somente é possível se c ou d é igual a 1. Logo,

$$p = cd \rightarrow p = 1 \cdot p \text{ ou } p = c \cdot 1$$

Então como (p) gera um ideal principal, e pela definição de ideal temos que

$$cd \in I \text{ e } dc \in I \rightarrow \text{ se } c=1 \text{ então } d \in I \text{ e } p = cd \rightarrow p = d$$

E o ideal gerado por (p) possui "identidade multiplicativa" 1. Ou seja, existe 1 em R .