1. **(4,0)** Seja R um anel comutativo com unidade e seja $R[X]$ o anel de polinômios com coeficientes em R. Mostre que :

   (a) O anel R é isomorfo ao anel $R[X]/\langle X\rangle$.

   (b) O ideal $\langle X\rangle$ de $R[X]$ é um ideal primo, se e somente se, R é um domínio de integridade.

   (c) O anel de polinômios $R[X]$ é um Domínio de Ideais Principais se, e somente se, R é corpo.

   (d) Em $\mathbb{Z}_6[X]$, escreva X como um produto de dois polinômios de grau 1.

(a) Seja $\varphi_0 : R[x] \longrightarrow R$ definida por

$\varphi_0(f(x)) = f(0)$.

φ_0 é homomorfismo de anéis.

φ_0 é sobrejetora, pois dado $a \in R$,

$\underset{\underset{R[x]}{\cap}}{\varphi_0(a)} = a$.

$\operatorname{Ker} \varphi_0 = \{a_0 + a_1 x + \cdots + a_n x^n = f(x) \mid f(0) = a_0 = 0\}$

Assim $f(x) \in \operatorname{Ker} \varphi_0 \Leftrightarrow a_0 = 0 \Leftrightarrow$

$f(x) = x(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in \langle x\rangle$.

Portanto, pelo Teorema do Homomorfismo,

$R[x]/\langle x\rangle \cong R$. ∎

(b) Sabemos que:

" Se R é um anel comutativo com unidade, um ideal $P \neq R$ é primo se, e somente se, R/P é um domínio de integridade."

Usando esse resultado temos que

$\dfrac{R[x]}{\langle x\rangle} \cong R$ (pelo item (a)).

Portanto $\langle x\rangle$ é ideal primo se, e somente se R é domínio de integridade. ∎

(c) Sabemos que: "Se R é um anel comutativo com unidade, um ideal M de R, $M \neq R$ é maximal se, e somente se, R/M é corpo"

Seja $R[X]$ um DIP. Pelo item (b), o ideal $\langle x \rangle$ de $R[X]$ é primo (só pelo fato de R ser domínio.)

($\Rightarrow$) Se $R[X]$ é DIP, $\langle X \rangle$ ideal primo de $R[X]$

$\Rightarrow \langle X \rangle$ maximal $\Rightarrow \dfrac{R[X]}{\langle X \rangle} \simeq R$ é corpo.

($\Leftarrow$) Se R for um corpo, então $R[X]$ é euclidiano $\Rightarrow R[X]$ é DIP. Pelo item (a) $\dfrac{R[X]}{\langle X \rangle} \cong \underset{\text{corpo}}{\underbrace{R}}$

$\Rightarrow \langle X \rangle$ é maximal. $\blacksquare$

(d) $$X = \underbrace{(\overline{3}X + \overline{4})}_{\neq 0}\underbrace{(\overline{4}X + \overline{3})}_{\neq 0} = \overline{12}X^2 + (\overline{16} + \overline{9})X + \overline{12}$$

Note $X \in \mathbb{Z}_6[X]$ não é primo.

$X \mid (\overline{3}X+\overline{4})(\overline{4}X+\overline{3})$, mas

$X \nmid \overline{3}X + \overline{4}$ e $X \nmid \overline{4}X + \overline{3}$.

(Verifique!)

2. **(3,0)**Seja $p \in \mathbb{Z}$ um número primo. Seja

$$R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

(a) Mostre que R é um subanel de $\mathbb{Q}$.

(b) Mostre que R tem um único ideal maximal M.

(c) A qual corpo o anel quociente R/M é isomorfo? Qual é o isomorfismo?

(a) $\underset{\frac{0}{1}}{0} \in R$, $1 \in R$

$\frac{0}{1}$ e $p \nmid 1$ $\frac{1}{1}$ e $p \nmid 1$.

Se $\frac{a}{b}$ e $\frac{c}{d} \in R$ então $p \nmid b$ e $p \nmid d$

$$\Rightarrow \frac{ad-bc}{\underbrace{bd}_{p \nmid bd}} = \frac{a}{b} - \frac{c}{d} \in R$$

Se $\frac{a}{b} \in R$ e $\frac{c}{d} \in R$ então $p \nmid b$ e $p \nmid d$

$\Rightarrow p \nmid bd \Rightarrow \frac{ac}{bd} \in R$.

(b) Seja J um ideal qualquer de R.

Se $J \neq \{0\}$, existe $\frac{a}{b} \in R$ com $p \nmid b$

e $a \neq 0$. Se $J \neq R$, então, $p \mid a$,

pois, se $p \nmid a$, $\frac{b}{a} \in R$ e $\frac{b}{a} \cdot \frac{a}{b} = 1 \in J$

e então $J = R$.

Se $M = \{ \frac{a}{b} \in R \mid p \mid a \}$, M é um ideal

(*) de R, $M \neq R$ e se J é um ideal

de R, então $J \subset M$.

É claro que M é maximal.

De fato, se $M \subsetneq I \subset R$,
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\;\;\hookrightarrow$ ideal

então existe $\frac{x}{y} \in I$ tq $p \nmid x \Rightarrow$

$\frac{y}{x} \in R \Rightarrow 1 \in I \Rightarrow I = R$.

Assim M é maximal.

E é o único pois se M' fosse ideal maximal $\underset{\text{por } (*)}{\Rightarrow} M' \subset M \Rightarrow M' = M$
$\hookrightarrow$ pois M' é maximal.

Observação

"No exercício 1 da Lista 4 era pedido para provar" se R é domínio de integridade P ideal primo de R. e $R_p = \{\frac{a}{b} \in K \mid b \notin P\}$, K corpo de frações de R, R_p tem um único ideal maximal M e $R_p/M \cong$ corpo de frações de $\frac{R}{P}$"

Se você leu esse enunciado, você sabe o que tem que provar aqui,

$R = \mathbb{Z}$, p primo, $P = \langle p \rangle$

$\mathbb{Z}_{\langle p \rangle}/M \cong$ corpo de frações de $\frac{\mathbb{Z}}{\langle p \rangle} \cong \mathbb{Z}_p$
$\downarrow$
corpo

No nosso caso então, mostrar que $R/M \cong \mathbb{Z}_p$.

Seja $\varphi : \mathbb{Z}_p \longrightarrow R/M$ $\quad\varphi$ é homomorfismo

$\varphi(a + \langle p \rangle) = \frac{a}{1} + M$

φ está bem definida e é injetora pois

$a + \langle p \rangle = b + \langle p \rangle \Leftrightarrow a - b \in \langle p \rangle$

$\Leftrightarrow p \mid (a-b) \Leftrightarrow \frac{a-b}{1} \in M \Leftrightarrow \frac{a}{1} - \frac{b}{1} \in M$

$\Leftrightarrow \frac{a}{1} + M = \frac{b}{1} + M$.

3. **(4,0)** Resolva **3** itens e já serão 4 pontos (se estiverem corretos).

(a) Mostre que o anel $\mathbb{Z}[\sqrt{-3}]$ não é um Domínio de Fatoração Unica.

(b) Mostre que $\mathbb{Z}[X]$ não é um domínio de ideais principais.

(c) Se D é um DIP, dados $a, b \in D$, existe um Máximo Divisor Comum de a e b e vale o Teorema de Bèzout.

(d) Se D é domínio de integridade, o polinômio $p(X) = X + a \in D[X]$ é primo em $D[X]$.

(a) Seja $\alpha = (1+\sqrt{-3})$. $N(\alpha) = \alpha\bar{\alpha} = 4$.

Então $4 = 2 \times 2 = \alpha\bar{\alpha}$.

Vamos mostrar que 2 é irredutível em $\mathbb{Z}[\sqrt{-3}]$.

Se $\exists\ a, b, c, d \in \mathbb{Z}$ tais que

$2 = (a+\sqrt{-3}\,b)(c+\sqrt{-3}\,d)$, então

$4 = (a^2+3b^2)(c^2+3d^2) \in \mathbb{Z}$

$2 \times 2 = (a^2+3b^2)(c^2+3d^2)$.

Poderíamos ter $a^2+3b^2 = 4$ e $c^2+3d^2 = 1$ ou

ou $a^2+3b^2 = 1$ e $c^2+3d^2 = 4$

$a^2+3b^2 = 2$ e $c^2+3d^2 = 1$

$a^2+3b^2 \geq 1$. Se $b \neq 0$ $a^2+3b^2 \geq 3$.

Logo $a^2+3b^2 = 1 \Rightarrow b = 0$.

Mas $b = 0$, $\Rightarrow 2 = a(c+\sqrt{-3}\,d) \Rightarrow ac = 2$

e $d = 0 \Rightarrow ac = 2 \Rightarrow a = 2$ e $c = 1$ ou

$a = 1$ e $c = 2$

Analogamente, para c^2+3d^2.

Só poderíamos então ter

$a^2+3b^2 = 2$ e $c^2+3d^2 = 2$

Se $b \neq 0$, $a^2+3b^2 \geq 3 \Rightarrow b = 0$. Mas $b = 0$,

$\Rightarrow a^2 = 2$. Mas $\sqrt{2} \notin \mathbb{Z}$.

Assim, 2 é irredutível em $\mathbb{Z}[\sqrt{-3}]$.

Mas $2 \nmid (1+\sqrt{-3})$ e $2 \nmid 1-\sqrt{-3}$

Se $(1+\sqrt{-3}) = 2(a+\sqrt{-3}\,b)$

$\Rightarrow 2a = 1 = 2b$ — absurdo.

Assim 2 é irredutível, $2 \mid \alpha\bar{\alpha}$ mas $2 \nmid \alpha$ e $2 \nmid \bar{\alpha}$.

Existem elementos irredutíveis em $\mathbb{Z}[\sqrt{-3}]$ que não são primos. Logo $\mathbb{Z}[\sqrt{-3}]$ não é um DFU. ■

(b) Se $\mathbb{Z}[x]$ fosse um DIP, então, o ideal primo $\langle x \rangle$ seria maximal e o quociente $\frac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$ seria corpo. Mas $\mathbb{Z}$ não é corpo!
(Exercício 1)

(c) Considere $J = \langle a \rangle + \langle b \rangle$. Como D é DIP, $\exists\, d \in J$ tal que $J = \langle d \rangle$.

Vamos provar que d é mdc (a, b).

$d \in J \Rightarrow \exists\, x, y \in D$ tais que $d = ax + by$.

$a \in J$ e $b \in J$ pois $a = a.1 + b.0$
$b = a.0 + b.1$

Mas $a, b \in J. \Rightarrow d \mid a$ e $d \mid b$.

Se $d' \in D$ é tal que $d' \mid a$ e $d' \mid b$
$\Rightarrow d' \mid ax$ e $d' \mid by \Rightarrow d' \mid \underbrace{(ax+by)}_{=d}$.

Logo d é mdc (a, b) e vale o Teorema de Bèzout.

(d) D domínio de integridade.

Mostrar que $X+a$ é primo em $D[X]$.

Suponha que $f(x), g(x) \in D[X]$ e que $X+a \mid f(x)g(x)$. Então $f(x)g(x) = (x+a)h(x)$

Logo $f(-a)g(-a) = \underbrace{(-a+a)}_{0} h(-a) = 0$.

Assim $f(-a) = 0$ ou $g(-a) = 0$.

Como $X+a$ é um polinômio mônico, podemos usar o algoritmo da divisão e escrever

$$f(x) = (x+a)q(x) + r(x),$$ onde $r(x)=0$ ou grau $r = 0$. (pois é < 1), ou seja $r(x) = r$ é constante

$$f(-a) = (-a+a)q(a) + r$$

Se $f(-a) = 0 \Rightarrow r = 0$

$\Rightarrow x+a \mid f(x)$.

Analogamente se $g(-a) = 0$.

Logo $X+a \mid f(x)$ ou $X+a \mid g(x)$. ∎