1. **(2,5)**

(a) Sejam p e q números primos distintos. Mostre que os subanéis de $\mathbb{Z}$, $p\mathbb{Z}$ e $q\mathbb{Z}$ não são isomorfos como anéis.

(b) Seja $\mathbb{Z}_m$ o anel dos inteiros módulo m, onde $m \in \mathbb{Z}, m > 0$.

i. Mostre que o anel Z_m contém elementos nilpotentes não nulos se, e somente se, existe um número primo $p \in \mathbb{Z}$ tal que $p^2|m$.

ii. Determine os elementos nilpotentes de $\mathbb{Z}_{24}$.

(a) $q \neq p$, q e p primos

Suponha que $\varphi : p\mathbb{Z} \longrightarrow q\mathbb{Z}$ é um homomorfismo de anéis

$\varphi(p) = qn$, para algum $n \in \mathbb{Z}$.

$$\varphi(p^2) = \varphi(\underbrace{p + \cdots + p}_{p \text{ parcelas}}) = p\varphi(p) = pqn$$

$$\varphi(p^2) = \varphi(pp) = \varphi(p)\varphi(p) = q^2n^2$$

Logo $pqn = q^2n^2 \Rightarrow p = qn$.

Mas p é primo. e $q \neq 1$, $q|p \Rightarrow q = p$, absurdo

Logo não existe homomorfismo de anéis de $p\mathbb{Z}$ em $q\mathbb{Z}$.

(b) (i) ($\Rightarrow$) Suponha, por absurdo que $m = p_1 p_2 \cdots p_k$ onde $p_i \neq p_j$ se $i \neq j$ e p_i primo $\forall i$.

Seja x tq $\exists\ n > 1$ com $x^n \equiv 0 \pmod{m}$.

$\Rightarrow m | x^n \Rightarrow p_i | x \quad \forall\ i = 1, \dots, k \Rightarrow$

$p_1 \cdots p_k | x \Rightarrow x \equiv 0 \pmod{m}$.

Logo o único nilpotente em $\mathbb{Z}_m$ é $\overline{0}$.

($\Leftarrow$) Suponha agora que existe p primo tal que $p^2 | m$. Então $m = p^2 m_1$, $m_1 \in \mathbb{Z}$.

Se tomarmos $x = pm_1$, então $\overline{x} = \overline{0}$ e

$$x^2 = p^2 m_1^2 = (\underbrace{p^2 m_1}_{})m_1 = mm_1 \equiv 0 \pmod{m}$$

$\exists\ \overline{x} \neq \overline{0}$ e $\overline{x}^{2m} = \overline{0}$.

(ii) Nilpotentes em $\mathbb{Z}_{24}$

$$\{\overline{0}, \underbrace{\overline{6}, \overline{12}, \overline{18}}_{\text{não nulos}}\}$$

2. **(2,5)** Seja $p \in \mathbb{Z}$, $p > 0$ um número primo.

(a) Mostre que $\sqrt{p} \notin \mathbb{Q}$.

(b) Seja

$$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

i. Mostre que $\mathbb{Q}(\sqrt{p})$ é um corpo.

ii. Mostre que os únicos subcorpos de $\mathbb{Q}(\sqrt{p})$ são $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{p})$.

(a) Se $\sqrt{p} \in \mathbb{Q}$, existiriam $a, b \in \mathbb{Z}$, $b \neq 0$ e $\frac{a}{b} = \sqrt{p}$. Podemos supor que $mdc(a,b) = 1$.

Então $\frac{a^2}{b^2} = p \iff a^2 = pb^2$.

Logo $p \mid a^2 \underset{p \text{ primo}}{\Longrightarrow} p \mid a \Rightarrow a = a_1 p$, $a_1 \in \mathbb{Z}$

Então $a_1^2 p^2 = p b^2 \Rightarrow a_1^2 p = b^2 \Rightarrow p \mid b$.

Logo $p \mid a$ e $p \mid b$, contrariando o fato de $mdc(a,b) = 1$.

(b) Vamos provar que $\mathbb{Q}(\sqrt{p})$ é subcorpo de $\mathbb{R}$.

(1) $0 = 0 + 0\cdot\sqrt{p}$, $0 \in \mathbb{Q}$

(2) $1 = 1 + 0\sqrt{p}$, $1 \in \mathbb{Q}, 0 \in \mathbb{Q}$

$\Big\}$ $0, 1 \in \mathbb{Q}(\sqrt{p})$

(3) Se $(a+b\sqrt{p})$ e $(c+d\sqrt{p}) \in \mathbb{Q}(\sqrt{p})$ então

$(a+b\sqrt{p}) - (c+d\sqrt{p}) = (a-c) + (b-d)\sqrt{p} \in \mathbb{Q}(\sqrt{p})$

(4) Se $a+b\sqrt{p}$ e $c+d\sqrt{p} \in \mathbb{Q}(\sqrt{p})$, então

$(a+b\sqrt{p})(c+d\sqrt{p}) = \underbrace{(ac+bdp)}_{\in \mathbb{Q}} + \underbrace{(ad+bc)}_{\in \mathbb{Q}}\sqrt{p} \in \mathbb{Q}(\sqrt{p})$

(5) Se $a+b\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ e $a+b\sqrt{p} \neq 0$, então, temos que mostrar que $(a+b\sqrt{p})^{-1} \in \mathbb{Q}(\sqrt{p})$.

Note que $(a+b\sqrt{p})(a-b\sqrt{p}) = a^2 - pb^2$,

$a+b\sqrt{p} \neq 0 \iff a^2 - pb^2 \neq 0$

Pois $a^2 - pb^2 = 0$ e $a = 0 \Rightarrow b = 0$
$b = 0 \Rightarrow a = 0$

E se $a \neq 0$ e $b \neq 0$, $a^2 - pb^2 = 0 \Rightarrow$
$p = \frac{a^2}{b^2} \in \mathbb{Q}$, absurdo

Basta ver que

$$(a+b\sqrt{p})^{-1} = \underbrace{\frac{a}{a^2-b^2p}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2-b^2p}}_{\in \mathbb{Q}}\sqrt{p} \in \mathbb{Q}(\sqrt{p})$$

(c) $\mathbb{Q}$ é corpo e $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$

$a \in \mathbb{Q}$, $a = a + 0\sqrt{p}$.

Seja K um subcorpo de $\mathbb{Q}(\sqrt{p})$. Então $0, 1 \in K$, e $n.1 \in K \ \forall n \in \mathbb{Z}$.

Assim $\mathbb{Z} \subset K$. Além disso, se $n \neq 0$, e como K e corpo, $\frac{1}{n} \in K$. Assim

$m.\frac{1}{n} \in K$, para todo $m, n \in \mathbb{Z}$, $m \neq 0$.

Logo $\mathbb{Q} \subset K$.

Se $K \neq \mathbb{Q}$, existe $a + b\sqrt{p} \in K$ com $b \neq 0$.

Logo $\underbrace{a + b\sqrt{p}}_{K} - \underset{\underset{K}{\cap}}{a} = b\sqrt{p} \in K$.

Como $b \neq 0$, $\frac{1}{b} b\sqrt{p} \in K \Rightarrow \sqrt{p} \in K$.

Assim $c + d\sqrt{p} \in K \ \forall c, d \in \mathbb{Q}$ e então $K = \mathbb{Q}(\sqrt{p})$ ∎

3. **(2,0)** Seja R um anel comutativo com unidade e seja $M \neq R$ um ideal de R. Mostre que M é um ideal maximal de R e, e somente se, o anel quociente R/M é um corpo.

($\Rightarrow$) $M \neq R$ e M ideal maximal.

Mostrar que R/M é corpo.

Como $M \neq R$, $\exists x \in R$ e $x \notin M$ então

$x + M \neq 0 + M = \bar{0}$.

Mostrar que existe $(x+M)^{-1}$.

$x \notin M$. Seja $J = xR + M$.

J é um ideal de R, $J \underset{\neq}{\supset} M$ (pois $x \notin M$).

Como M é maximal, $J = R$. Assim, existem $y \in R$ e $m \in M$ tais que $1 = xy + m \Rightarrow 1 - xy = m$

$xy \equiv 1 \pmod{M} \Rightarrow (x+M)(y+M) = \underline{1}$.

($\Leftarrow$) Suponha agora que R/M é corpo.

Mostrar que M é maximal.

Suponha que $M \underset{\neq}{\subset} J \subset R$ ↳ ideal

Se $M \neq J$, então existe $x \in J$ tal que $x \notin M$. Como R/M é corpo, existe $y \in R$ tal que $(x+M)(y+M) = 1 + M$

$(xy + M) = 1 + M$.

$\Rightarrow \underbrace{xy}_{\in J} - 1 \in M$ é $\in R$

$xy \in J$, $xy - 1 \in M \subset J$

$\Rightarrow 1 \in J \Rightarrow J = R$.

Logo M é ideal maximal de R.

4. **(3,0)** Seja R um anel comutativo com unidade. Sejam M e N ideais maximais de R com $M \neq N$.

(a) Mostre que $M + N = R$.

(b) Mostre que a função $f : R \to R/M \times R/N$, definida por $f(x) = (x + M, x + N)$, é um homomorfismo de anéis e é sobrejetora.

(c) Mostre que $R/M \cap N$ é isomorfo a $R/M \times R/N$.

(a) Como $M \neq N$, $\exists\, x \in N$ tal que $x \notin N$. Então $M + xR$ é um ideal de R, $M + xR \neq M$ e M é maximal e $M + xR \supset M$. Logo $M + xR = R$. Como $M + xR \subset M + N$ tem-se que $R \subset M + N \Rightarrow M + N = R$. $\square$

(b) $f : R \longrightarrow R/_M \times R/_N$

$f(x) = (x + M, x + N)$

É claro que f é homo de anéis

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

$f(xy) = (xy + M, xy + N) = (x+M, x+N)(y+M, y+N)$

Mostrar que f é sobrejetora.

Seja $(a+M, b+N) \in R/_M \times R/_N$.

Mostrar que existe $x \in R$ tq $(x+M, x+N) = (a+M, b+N)$.

Como $M + N = R$, $a = a_1 + a_2$, onde $a_1 \in M$ e $a_2 \in N$.

Então $(a - a_2) = a_1 \in M \Rightarrow a + M = a_2 + M$.

Analogamente, $b = b_1 + b_2$, $b_1 \in M$ e $b_2 \in N$, $b + N = b_1 + N$.

Se $x = a_2 + b_1$, então $x + M = a_2 + M = a + M$
$x + N = b_1 + N = b + M$.

(c) Basta usar o Teorema do Homomorfismo

$$R/_{\mathrm{Ker} f} \cong \mathrm{Im}\, f = \frac{R}{M} \times \frac{R}{N}$$

e $\mathrm{Ker} f = \{x \in R \mid (x+M, x+N) = (\bar{0}, \bar{0})\}$

$\Leftrightarrow x \in M$ e $x \in N \Leftrightarrow x \in M \cap N$.

Assim $\dfrac{R}{M \cap N} \cong \dfrac{R}{M} \times \dfrac{R}{N}$.