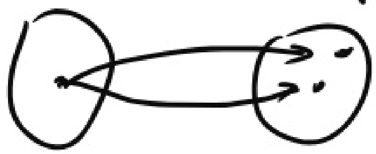
Monitoria:

não é função



Ex 5

1) Queremos provar que se $m \mid n$

$$f: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$$
$$\bar{x} \longmapsto \bar{x}$$

está bem definida. Considere $\bar{a} = \bar{b} \iff a \equiv b \pmod{n} \iff n \mid a-b$. Como $m \mid n$, temos que $m \mid a-b \iff a \equiv b \pmod{m} \iff \bar{a} = \bar{b}$ (em $\mathbb{Z}_m$)

$a \equiv b \pmod{m} \iff \bar{a} = \bar{b}$ (em $\mathbb{Z}_m$) $\iff$

$f(\bar{a}) = f(\bar{b})$.

$\blacksquare$

Ex 6:

(1) Queremos mostrar que

$$\begin{aligned} f : \mathbb{Z}_{mn} &\longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \\ \bar{x} &\longmapsto (\bar{x}, \bar{x}) \end{aligned}$$

está bem definida.

Considere $\bar{a} = \bar{b}$ (em $\mathbb{Z}_{mn}$) $\Leftrightarrow$

$a \equiv b \pmod{mn} \Leftrightarrow mn \mid (a-b) \Leftrightarrow$

$m \mid (a-b)$ e $n \mid (a-b)$, pois $m \mid mn$ ($n \mid mn$)

e recíproco vale pois $mdc(m,n) = 1$.

Então como $m \mid (a-b) \Leftrightarrow a \equiv b \pmod{m}$

$\Leftrightarrow \bar{a} = \bar{b}$ (em $\mathbb{Z}_m$)

Analogamente, $\bar{a} = \bar{b}$ (em $\mathbb{Z}_n$).

Assim $f(\bar{a}) = (\bar{a}, \bar{a}) = (\bar{b}, \bar{b}) = f(\bar{b})$

$\blacksquare$

item 5) Como $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$, basta provar que f é injetora (ie, $x \neq y \Rightarrow f(x) \neq f(y)$). Usando a contrapositiva, se $f(a) = f(b) \Rightarrow (\bar{a}, \bar{a}) = (\bar{b}, \bar{b}) \Rightarrow$ $\bar{a} = \bar{b}$ (em $\mathbb{Z}_m$) e $\bar{a} = \bar{b}$ (em $\mathbb{Z}_n$) $\Rightarrow$

$\bar{a} = \bar{b}$ (em $\mathbb{Z}_m$) e $\bar{a} = \bar{b}$ (em $\mathbb{Z}_n$)

Logo, $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$

donde $m \mid (a-b)$ e $n \mid (a-b)$. Assim,

como $mdc(m,n) = 1$, $mn \mid a-b \Rightarrow$

$a \equiv b \pmod{mn} \Rightarrow \bar{a} = \bar{b}$ (em $\mathbb{Z}_{m \cdot n}$)

$\blacksquare$

Ex3: Considere A um anel finito, não trivial (i.e, $A = \{0\}$). Suponha que $\forall a, b, c \, (a \leq b \Rightarrow a + c \leq b + c)$.

Como $\leq$ é uma ordem total, podemos escrever $A = \{a_1 \leq \cdots \leq a_m\}$. Assim, para $a_k \in A$

$$\underbrace{a_m + a_k}_{\in A} \leq a_m \Rightarrow -a_m + (a_m + a_k) \leq -a_m + a_m$$

$a_m + a_k \leq a_m \Rightarrow -a_m + (a_m + a_k) \leq$

$-a_m + a_m \Rightarrow a_k \leq 0 \ (*)$

Ou seja, concluímos que todo elemento de A satisfaz $(*)$. No entanto, para todo $a_k \neq 0$, se $a_k \leq 0$ então

$-a_k \geq 0$

$a_k \leq 0 \Rightarrow -a_k + a_k = 0 \leq -a_k$

Assim, chegamos a uma contradição com (*). $\blacksquare$