Math 3450
4/18/24

$\boxed{\text{HW 3}}$

7. In $\mathbb{Z}_n$ is $\overline{a} \oplus \overline{b} = \overline{a^b}$ well-defined?

No.

<u>Reason 1:</u> $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$\overline{2} \oplus \overline{-1} = \overline{2^{-1}} = \overline{\left(\frac{1}{2}\right)}$ ← <u>that's not in $\mathbb{Z}_4$!</u>

<u>Reason 2:</u> $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$\overline{1} = \overline{5}$

To be well-defined we would need $\overline{2} \oplus \overline{1} = \overline{2} \oplus \overline{5}$

But, $\overline{2} \oplus \overline{1} = \overline{2^1} = \overline{2}$

$\overline{2} \oplus \overline{5} = \overline{2^5} = \overline{32} = \overline{0}$

not equal

⑧ (e) $\mathbb{N} = \{1, 2, 3, \ldots\}$

$S = \mathbb{N} \times \mathbb{N} = \{(1,1), (1,2), (2,1), \ldots\}$

Define $(a,b) \sim (c,d)$ means

$a + d = b + c$. $\leftarrow$ $\boxed{a - b = c - d}$

Ex: $(1,2) \sim (4,5)$ since $1+5 = 2+4$

$(1,2) \sim (7,8)$ since $1+8 = 2+7$

You show $\sim$ is an equiv. relation

$\overline{(1,2)} = \{(1,2), (2,3), (3,4), (4,5), \ldots\}$

$\overline{(3,8)} = \{(1,6), (2,7), (3,8), (4,9), \ldots\}$

$\overline{(8,8)} = \{(1,1), (2,2), (3,3), (4,4), (5,5), \ldots\}$

Define $\oplus$ on $S/\sim$ on the set of equivalence classes:

$$\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c,\ b+d)}$$

Ex: $\overline{(1,2)} \oplus \overline{(3,8)} = \overline{(4,10)}$

$\overline{(2,3)} \oplus \overline{(2,7)} = \overline{(4,10)}$

Prove $\oplus$ is well-defined:

① Let $\overline{(a,b)}, \overline{(c,d)}$ be two equivalence classes.

Since $(a,b),(c,d) \in S$ we know $a,b,c,d \in \mathbb{N}$.

So, $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c,b+d)}$ is still a valid equvalence class since $a+c, b+d \in \mathbb{N}$.

② Suppose $\overline{(a,b)} = \overline{(x,y)}$ and

$$\overline{(c,d)} = \overline{(m,n)}.$$

We need to show that

$$\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$$

is equal to

$$\overline{(x,y)} \oplus \overline{(m,n)} = \overline{(x+m, y+n)}$$

Since $\overline{(a,b)} = \overline{(x,y)}$ we know $a-b = x-y$.

Since $\overline{(c,d)} = \overline{(m,n)}$ we know $c-d = m-n$.

Thus,

$$\begin{aligned}(a+c)-(b+d) &= (a-b)+(c-d)\\ &= (x-y)+(m-n)\\ &= (x+m)-(y+n)\end{aligned}$$

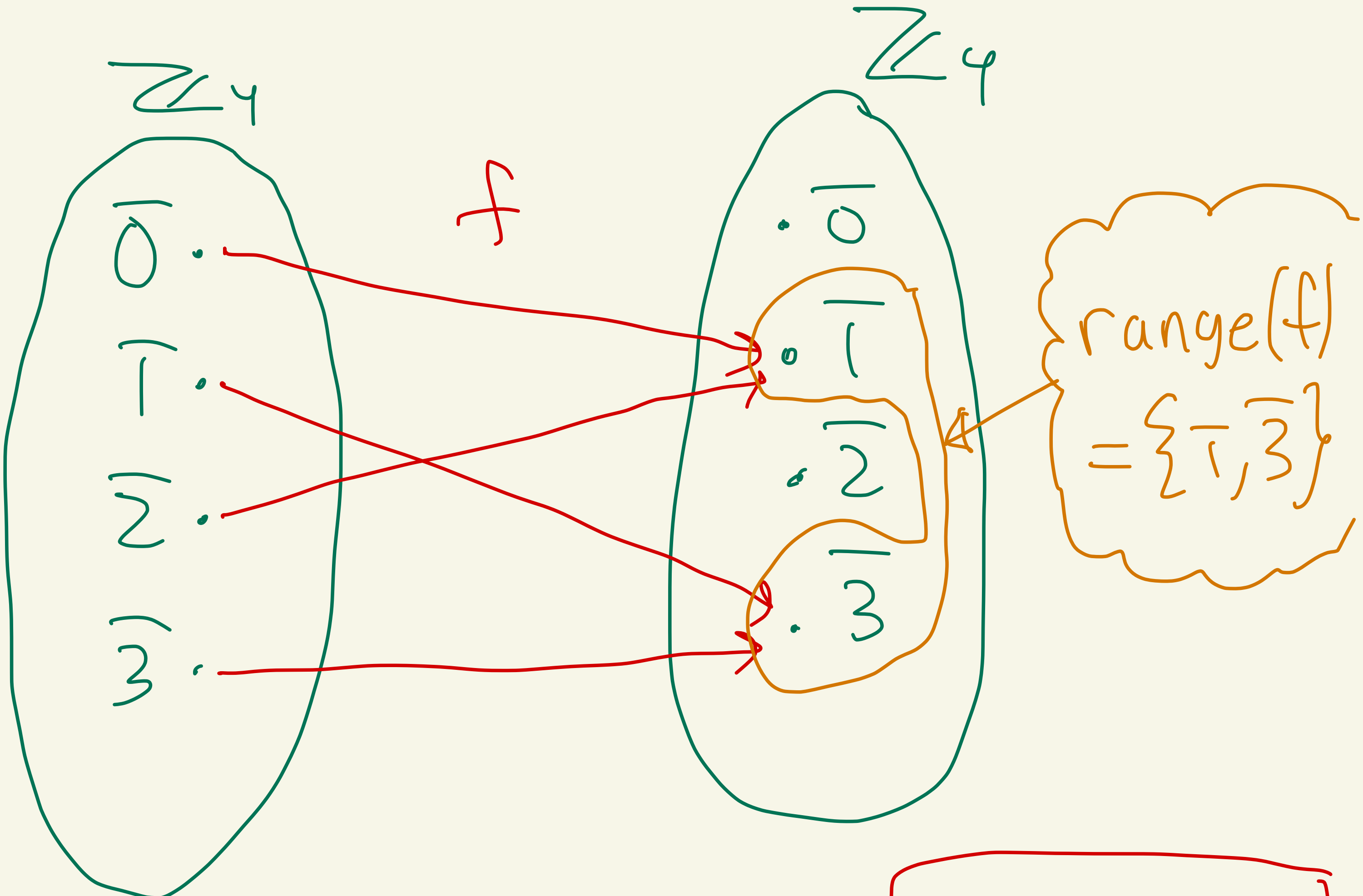
Therefore, $\overline{(a+c, b+d)} = \overline{(x+m, y+n)}$.

$\blacksquare$

$\boxed{\text{HW 4}}$

(2) (e) $f : \mathbb{Z}_4 \to \mathbb{Z}_4$

$$f(\overline{x}) = \overline{2} \cdot \overline{x} + \overline{1}$$



$$f(\overline{0}) = \overline{2} \cdot \overline{0} + \overline{1} = \overline{1}$$

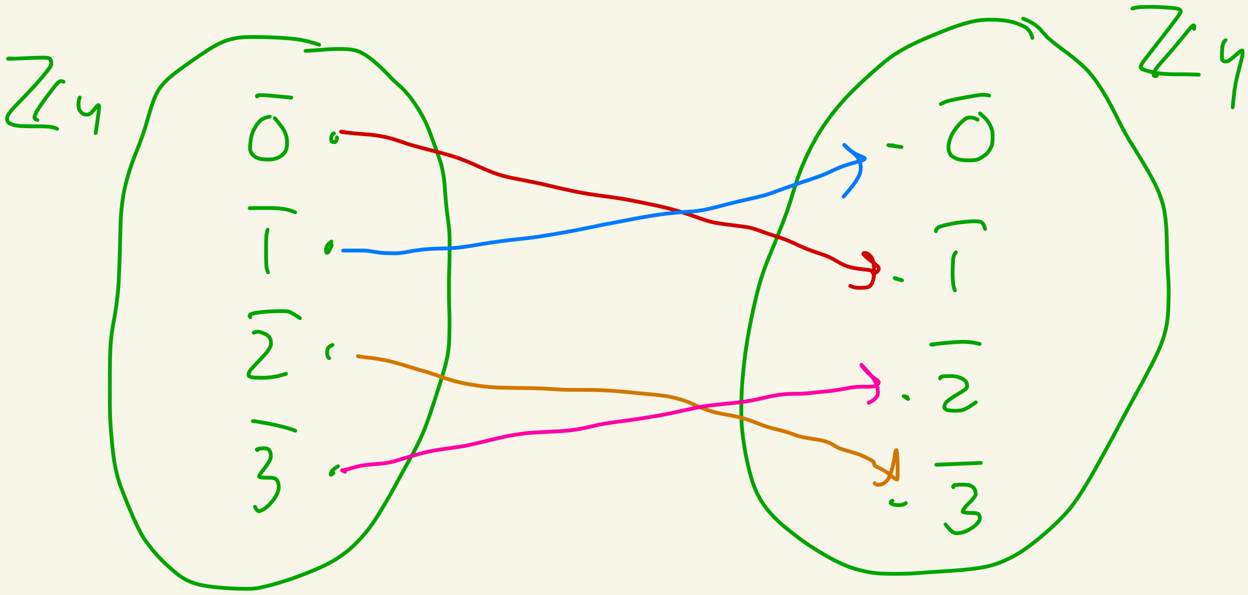
$$f(\overline{1}) = \overline{2} \cdot \overline{1} + \overline{1} = \overline{3}$$

$$f(\overline{2}) = \overline{2} \cdot \overline{2} + \overline{1} = \overline{5} = \overline{1}$$

$$f(\overline{3}) = \overline{2} \cdot \overline{3} + \overline{1} = \overline{7} = \overline{3}$$

$\boxed{\begin{array}{l} f \text{ not } 1\text{-}1 \\ f \text{ not onto} \end{array}}$

$g: \mathbb{Z}_4 \to \mathbb{Z}_4, \quad g(\overline{x}) = \overline{3}\,\overline{x} + \overline{1}$



g is 1-1 and onto.

What is g^{-1}?

Solve for $\overline{x}$ in $\overline{y} = \overline{3}\,\overline{x} + \overline{1}$.

$$\overline{y} = \overline{3}\,\overline{x} + \overline{1}$$

add $\overline{3}$

$\overline{1} + \overline{3} = \overline{0}$

$$\overline{y} + \overline{3} = \overline{3}\,\overline{x}$$

$\times\, \overline{3}$

$$\overline{3}\,\overline{y} + \overline{9} = \overline{9}\,\overline{x}$$

$\overline{9} = \overline{1}$

$$\overline{3}\,\overline{y} + \overline{1} = \overline{x}$$

So, $\bar{g}^{-1}(\bar{x}) = \bar{3}\,\bar{x} + \bar{1}$ ← interchange $\bar{x}$ & $\bar{y}$

So, $g = g^{-1}$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

$\boxed{\text{HW 4}}$

9. Let $f: A \to B$, $g: B \to C$.
If f is not one-to-one, then $g \circ f$ is not one-to-one.

> If P, then Q
> is equivalent to
> If $\neg Q$, then $\neg P$.
>
> contrapositive

Contrapositive of above:

$$\boxed{\text{If } g \circ f \text{ is one-to-one, then } f \text{ is one-to-one}}$$

<u>proof:</u>

Assume $g \circ f$ is one-to-one.
Let's show this implies that f is one-to-one.

Suppose that $f(a_1) = f(a_2)$.

So, $g(f(a_1)) = g(f(a_2))$

That is, $(g \circ f)(a_1) = (g \circ f)(a_2)$

Then, $a_1 = a_2$ since $g \circ f$ is 1-1.

Thus, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

So, f is 1-1. $\blacksquare$

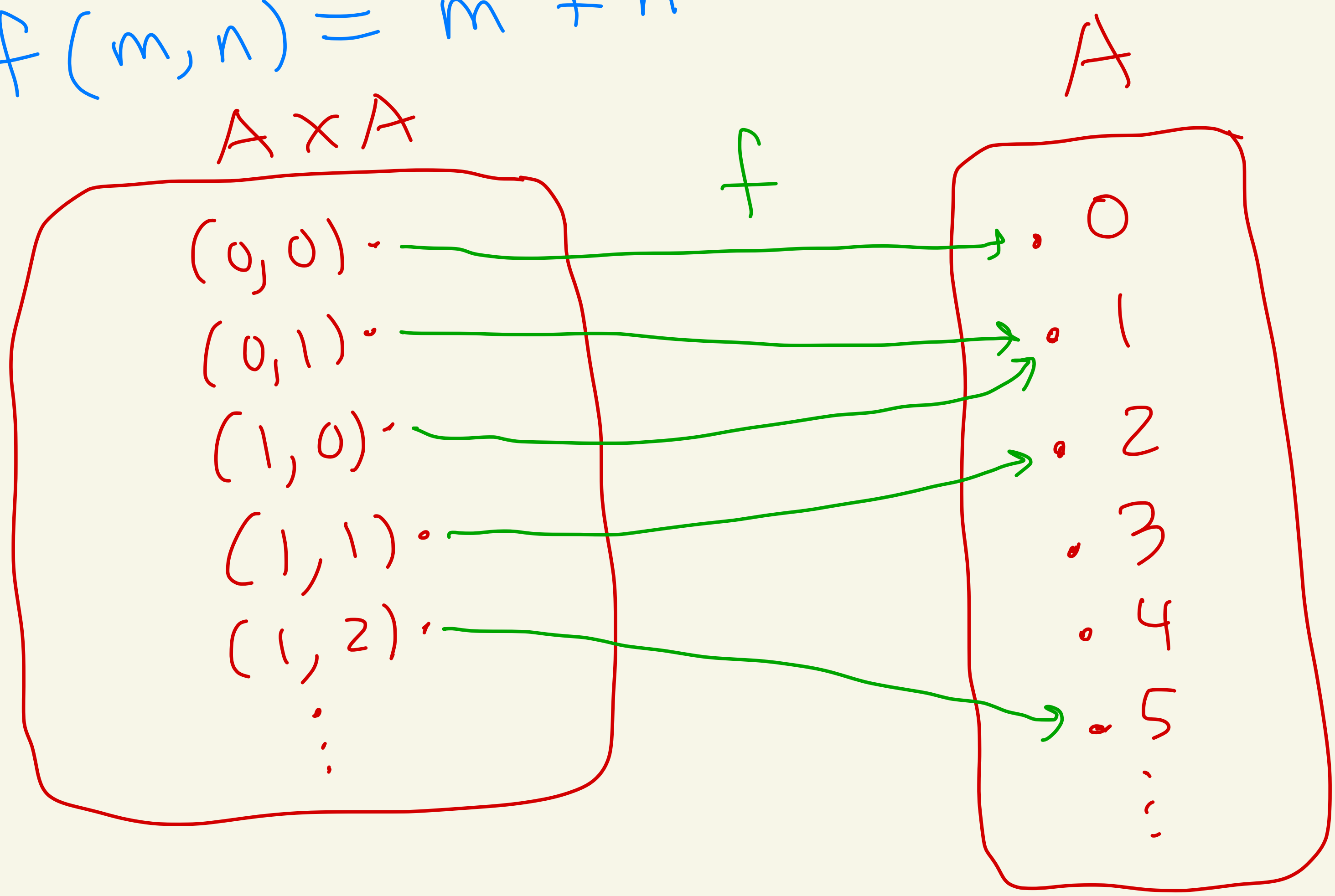
---

12 (HW 4)

$A = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, \ldots\}$

$f : A \times A \to A$

$f(m,n) = m^2 + n^2$



(d) Show f is not 1-1

$$\boxed{\begin{array}{l}\text{Since } f(0,1) = 1 = f(1,0) \\ \text{and } (0,1) \neq (1,0) \text{ we} \\ \text{Know } f \text{ is not } 1\text{-}1.\end{array}}$$

(e) Show f is not onto

There is no (m,n) with $f(m,n) = 3$ ie with $m^2 + n^2 = 3$.

See with table:

(m,n)	m^2+n^2
$(0,0)$	0
$(1,0)$	1
$(0,1)$	1

$(1,1)$	2
$(0,2)$	4
$(2,0)$	4
$(1,2)$	5
$(2,1)$	5
$\vdots$	$\vdots$

always greater than 3