Weds
10/16

HW 3

#4 Define $\bar{a} \oplus \bar{b} = \bar{a}^2 + \bar{b}^2$ on $\mathbb{Z}_n$.

Prove $\oplus$ is a well-defined operation on $\mathbb{Z}_n$.

$$4 \overset{3}{\overline{)13}} \quad -12 \quad \boxed{1}$$

remainder

$\overline{13} = \bar{4} \cdot \bar{3} + \bar{1}$

$= \bar{0} \cdot \bar{3} + \bar{1}$

$= \bar{1}$

Ex: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{4} = \bar{0}$

$\overline{13} = \overline{13} + \overline{-4} + \overline{-4} + \overline{-4}$

$= \bar{1}$

$\bar{2} \oplus \bar{3} = \bar{2}^2 + \bar{3}^2 = \bar{4} + \bar{9} = \overline{13} = \bar{1}$

proof that $\oplus$ is well-defined on $\mathbb{Z}_n$

① Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$ where $a, b \in \mathbb{Z}$.

Then,

$$\bar{a} \oplus \bar{b} = \bar{a}^2 + \bar{b}^2 = \bar{a}\cdot\bar{a} + \bar{b}\cdot\bar{b}$$
$$= \overline{a^2} + \overline{b^2}$$
$$= \overline{a^2 + b^2}$$

And $a^2 + b^2 \in \mathbb{Z}$.

So, $\bar{a} \oplus \bar{b} = \overline{a^2 + b^2} \in \mathbb{Z}_n$.

Thm from class | In $\mathbb{Z}_n$:

If $\bar{x} = \bar{y}$ and $\bar{w} = \bar{z}$ then

$$\bar{x} + \bar{w} = \bar{y} + \bar{z}$$
$$\bar{x} \cdot \bar{w} = \bar{y} \cdot \bar{z}$$

② Let $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n$

where $\bar{a} = \bar{c}$ and $\bar{b} = \bar{d}$.

We need to show that $\bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$.

From a theorem in class, since $\bar{a} = \bar{c}$

we know $\bar{a}^2 = \bar{c}^2$.

Also since $\bar{b} = \bar{d}$ we get $\bar{b}^2 = \bar{d}^2$.

Since $\bar{a}^2 = \bar{c}^2$ and $\bar{b}^2 = \bar{d}^2$ we get

$$\bar{a}^2 + \bar{b}^2 = \bar{c}^2 + \bar{d}^2.$$

So, $\bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$. □

Def: Let A and B be sets and $f : A \to B$.

We say that f is one-to-one or injective if

for every $a_1, a_2 \in A$ we have that the following is true:

If $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

contrapositive: If $f(a_1) = f(a_2)$, then $a_1 = a_2$.

this means: f is a function with

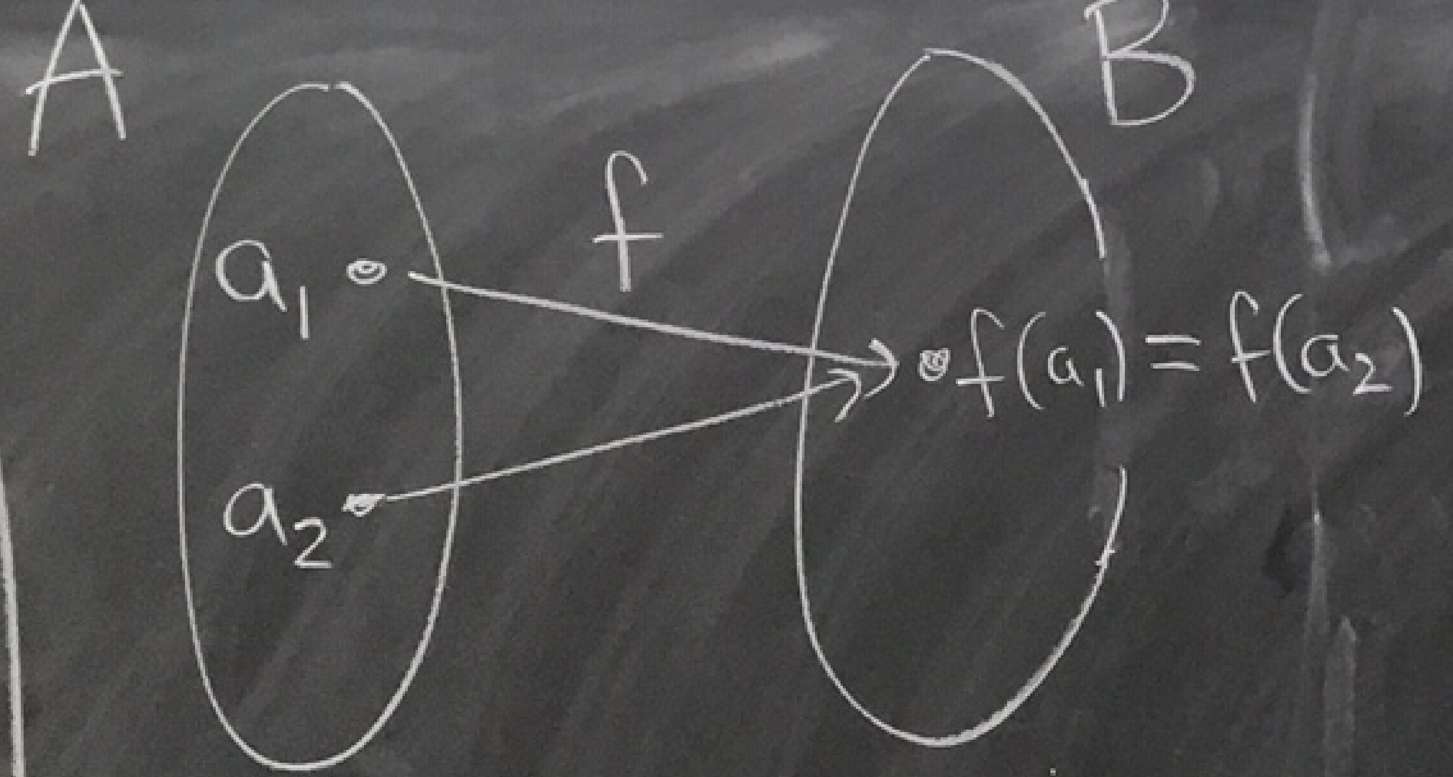
input → domain$(f) = A$

output → codomain$(f) = B$

If P, then Q

Contrapositive: If $\neg Q$, then $\neg P$.

A



not one-to-one if $a_1 \neq a_2$

How to prove $f : A \to B$ is one-to-one

Let $a_1, a_2 \in A$.

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

$\vdots$ (proof stuff)

Conclude that $a_1 = a_2$.

Ex: Let $f: \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 10x + 1$.

Note that f is well-defined since $f(x) = 10x + 1 \in \mathbb{R}$ for every $x \in \mathbb{R}$

Then f is one-to-one.

pf: Let $a, b \in \mathbb{R}$.

Suppose $f(a) = f(b)$.

Then $10a + 1 = 10b + 1$

So, $10a = 10b$.

Thus, $a = b$.

Therefore, f is one-to-one. ∎

Ex:

$f: \mathbb{R} \to \mathbb{R}$

$f(x) = \frac{1}{x}$

f is not well-defined since $0 \in \mathbb{R} \leftarrow \boxed{\text{domain}}$

but $f(0) = \frac{1}{0} \notin \mathbb{R} \leftarrow$ codomain f($\bar{6}$)

<u>Ex:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$.
Define $f: \mathbb{Z}_n \to \mathbb{Z}_n$ by
$f(\bar{x}) = \bar{x}^2$.

<u>f is well-defined</u>

① Let $\bar{x} \in \mathbb{Z}_n$ where $x \in \mathbb{Z}$.
Then,
$$f(\bar{x}) = \bar{x}^2 = \bar{x} \cdot \bar{x} \in \mathbb{Z}_n.$$

② Suppose $\bar{x_1} = \bar{x_2}$ where $x_1, x_2 \in \mathbb{Z}$.
Then,
$$f(\bar{x_1}) = \bar{x_1}^2 = \bar{x_2}^2 = f(\bar{x_2}).$$
Thm from class. Multiply $\bar{x_1} = \bar{x_2}$ and $\bar{x_1} = \bar{x_2}$

$\blacksquare$

Ex: $f: \mathbb{Z}_7 \to \mathbb{Z}_7$ $\quad f(\bar{x}) = \bar{x}^2$

calculations

$f(\bar{3}) = \bar{3}^2 = \bar{9} = \bar{2}$

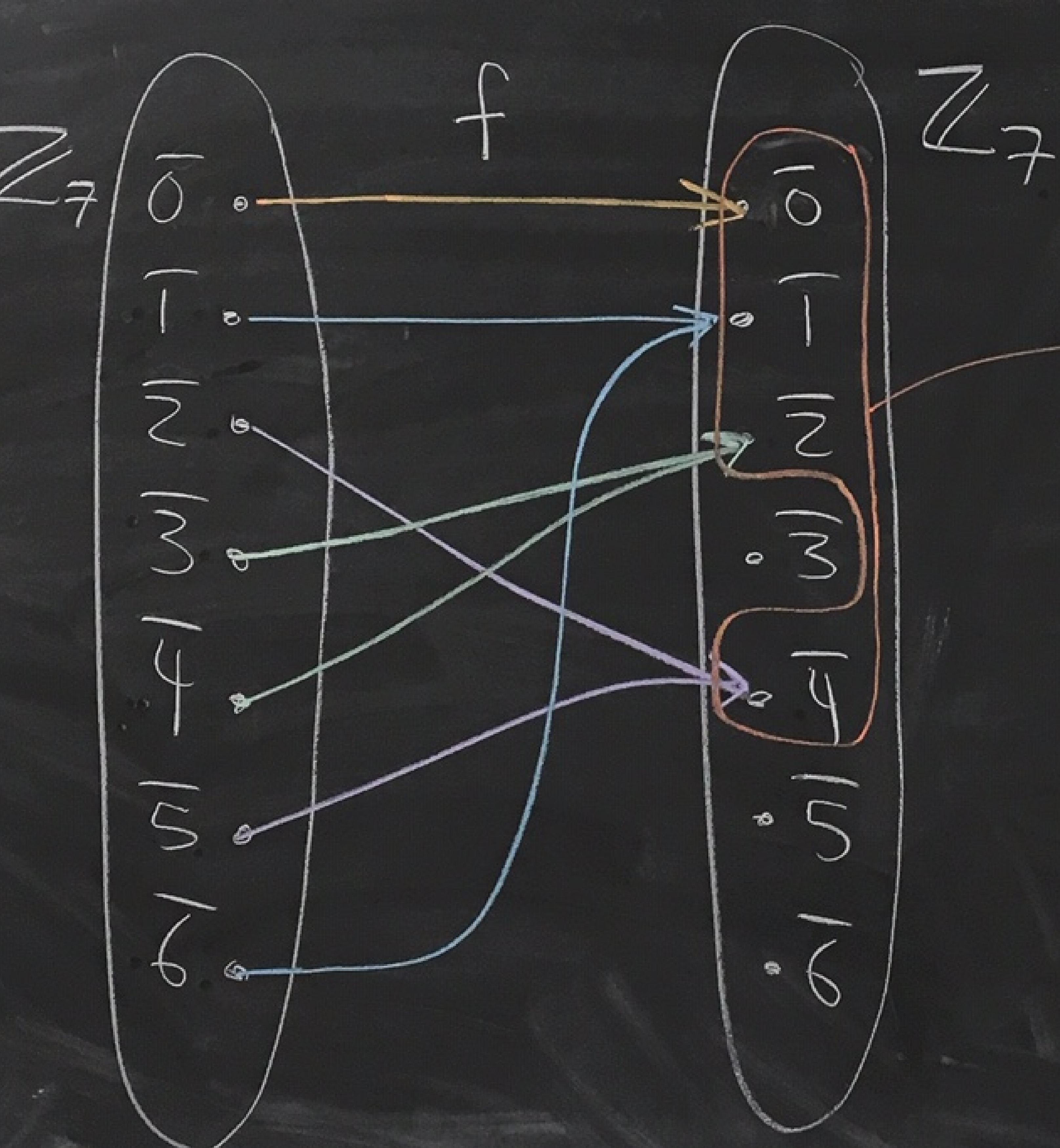
$f(\bar{4}) = \overline{16} = \bar{2}$

$\bar{5} = \overline{-2}$

$f(\bar{5}) = f(\overline{-2}) = \bar{4}$

$\bar{6} = \overline{-1}$

$f(\bar{6}) = f(\overline{-1}) = \bar{1}$



these are called quadratic residues

$\text{range}(f) = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$

f is not one-to-one

for example, $\bar{1} \neq \bar{6}$ but $f(\bar{1}) = f(\bar{6})$

$\boxed{\bar{6} = \overline{-1}}$

es

$= f(\bar{6})$

Ex: $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(\bar{x}) = \bar{x}^2$

f is <u>not</u> one-to-one if $n > 2$.

pf: If $n > 2$, then $\bar{1} \neq \overline{-1}$ in $\mathbb{Z}_n$.

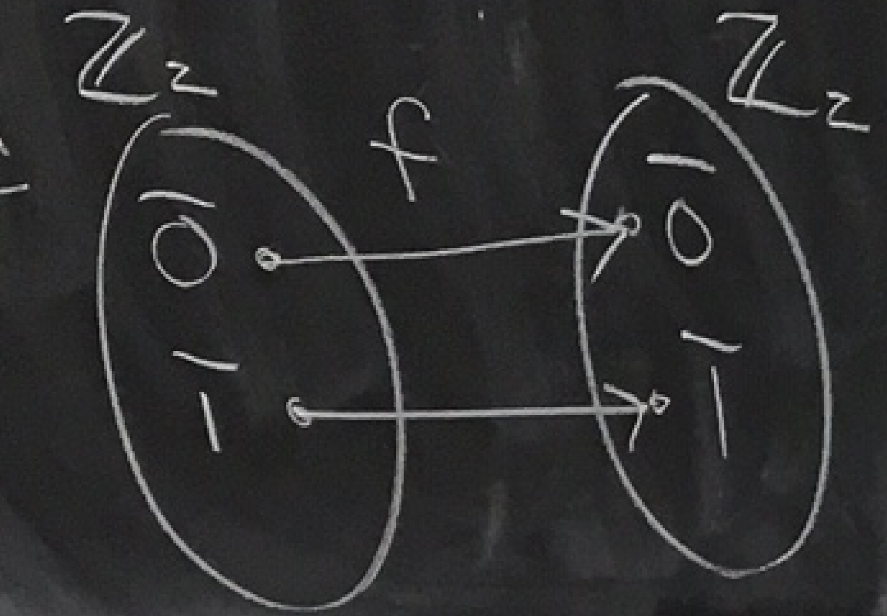
And, $f(\bar{1}) = \bar{1}^2 = \bar{1}$ and $f(\overline{-1}) = (\overline{-1})^2 = \bar{1}$.

So, f is not one-to-one if $n > 2$. ∎

Why is $\bar{1} \neq \overline{-1}$ when $n > 2$?

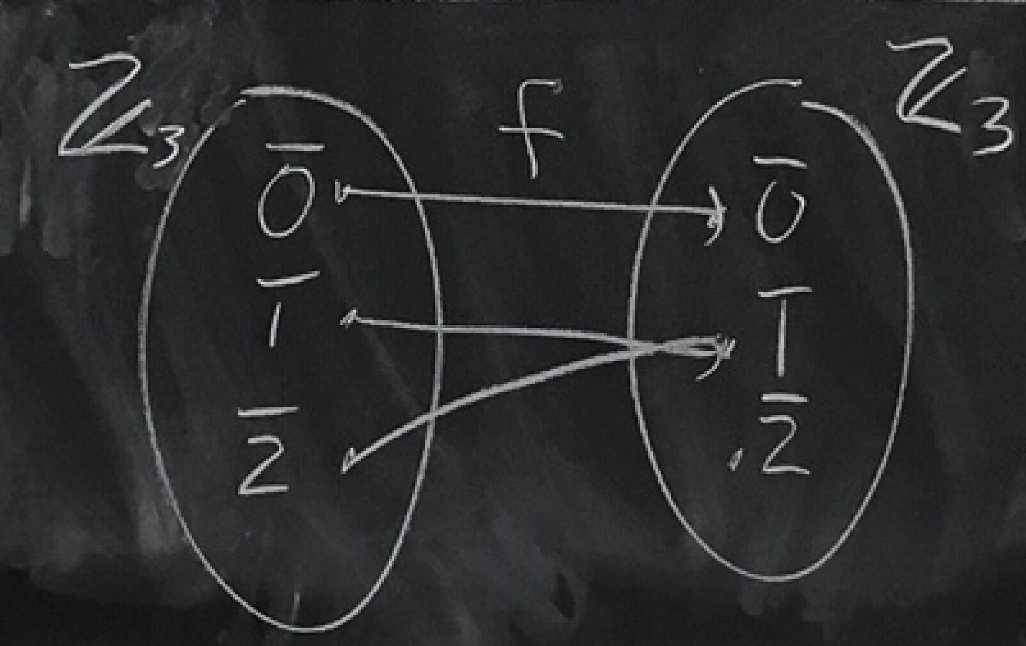
If $\bar{1} = \overline{-1}$ then
$1 \equiv -1 \pmod{n}$ and so
$n \mid (1 - (-1))$ or $n \mid 2$.
So, $n = \pm 1, \pm 2$

Ex:



$f : \mathbb{Z}_2 \to \mathbb{Z}_2$
$f(\bar{x}) = \bar{x}^2$
f is one-to-one

Ex:



$f : \mathbb{Z}_3 \to \mathbb{Z}_3$
$f(\bar{x}) = \bar{x}^2$
f is <u>not</u> one-to-one