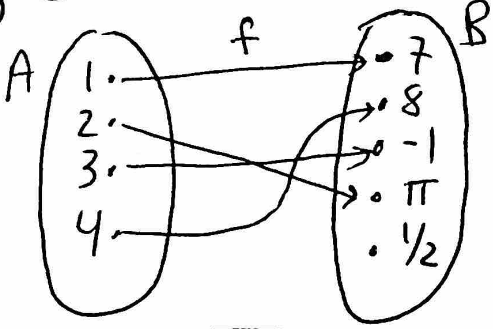
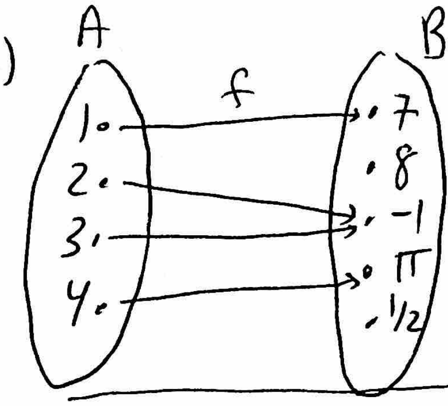
Homework 4 Solutions

1 (a)



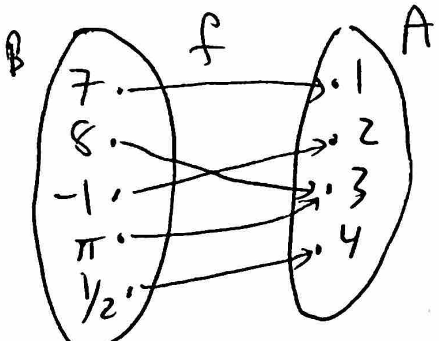
$\boxed{f \text{ is } 1\text{-}1}$

(b)



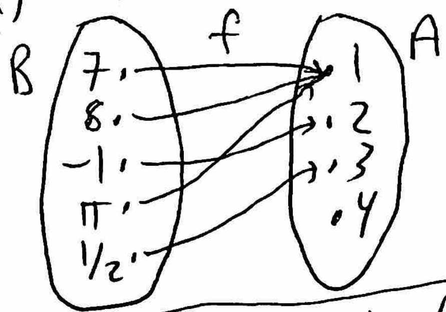
f is not 1-1 since $f(2)=f(3)$ and $2 \neq 3$

(c)



$\boxed{f \text{ is onto } A}$

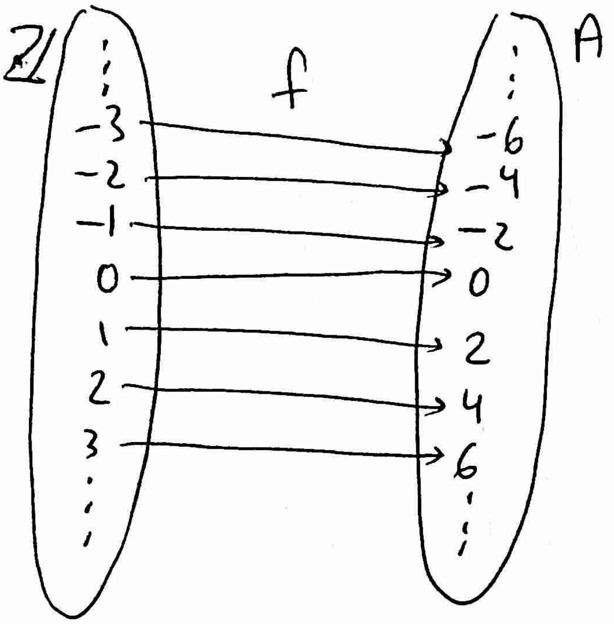
(d)



f is not onto A since $4 \in A$ and $\nexists b$ with $f(b)=4$

$\nexists$ means "there does not exist"

(2) (a) $f: \mathbb{Z} \to A$, $f(k) = 2k$, $A = \{2n \mid n \in \mathbb{Z}\}$



(i) f is one-to-one.
Suppose that $f(x) = f(y)$, for some $x, y \in \mathbb{Z}$. Then $2x = 2y$. Dividing by 2 gives $x = y$.

(ii) Let $y \in A$. Then $y = 2n$ for some $n \in \mathbb{Z}$. We have that $f(n) = 2n = y$. So for every $y \in A$ there exists $n \in \mathbb{Z}$ with $f(n) = y$. Thus f is onto.
Thus f is a bijection.

(iii) By (a) & (b) f is a bijection.
Solving $y = f(x)$ gives $y = 2x$ which gives $x = \frac{y}{2}$
Since y is even, $x = \frac{y}{2}$ is an integer. We have
$f^{-1}(y) = \frac{y}{2}$.

2(b) $f: \mathbb{Q} \to \mathbb{Q}$ where $f(x) = x^3$.

(i) f is one-to-one. Suppose $f(x) = f(y)$ where $x, y \in \mathbb{Q}$. Then $x^3 = y^3$. So, $(x^3)^{1/3} = (y^3)^{1/3}$. So, $x = y$.

(ii) f is not onto. We will show that 2 is not in the range of f. Suppose that there exists $\frac{a}{b} \in \mathbb{Q}$ with $f(\frac{a}{b}) = 2$. ~~Then $\frac{a}{b}$~~ We will assume that $\frac{a}{b}$ is in lowest terms and then arrive at a contradiction. Since $f(\frac{a}{b}) = 2$ we have
$(\frac{a}{b})^3 = 2$. So 2

So, $a^3 = 2b^3$. Thus, $2 \mid a^3$. This implies that a is even. Why?

Lemma: If $2 \mid x^3$ where $x \in \mathbb{Z}$, then x is even.
Pf: Suppose x is odd. Then $x = 2k+1$ where $k \in \mathbb{Z}$.
Then, $x^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2[4k^3 + 6k^2 + 3k] + 1$.
So, if x is odd then x^3 is odd. So if x is odd then $2 \nmid x^3$. Therefore, if $2 \mid x^3$ then x is even. $\square$

Since a is even, $a = 2l$ where $l \in \mathbb{Z}$.
Plugging this into $a^3 = 2b^3$ gives $2^3 l^3 = 2b^3$.
Then $2[2l^3] = b^3$. So, $2 \mid b^3$. Thus, again we have $2 \mid b$.

Therefore 2 is a common divisor of a & b and $\frac{a}{b}$ is not in lowest terms. Thus, there does not exist $\frac{a}{b} \in \mathbb{Q}$ with $\left(\frac{a}{b}\right)^3 = 2$.

(iii) f is not a bijection since f is not onto.

2(c) $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 5$

(i) f is one-to-one. Suppose $f(x) = f(y)$ for some $x, y \in \mathbb{R}$. Then $2x + 5 = 2y + 5$. Solving we get $x = y$.

(ii) f is onto. Given $b \in \mathbb{R}$ we ~~have that~~ need to find $a \in \mathbb{R}$ with $f(a) = b$. Trying to solve we have $2a + 5 = b$ or $a = \frac{b-5}{2}$.
$a = \frac{b-5}{2}$ is always in $\mathbb{R}$ for any $b \in \mathbb{R}$.
And $f\left(\frac{b-5}{2}\right) = 2\left(\frac{b-5}{2}\right) + 5 = b$.

(iii) f is bijective and $f^{-1}(x) = \frac{b-5}{2}$.

2(d) $f: \mathbb{R} \to \mathbb{R}$ with $f(x) = x^4 - 16$.

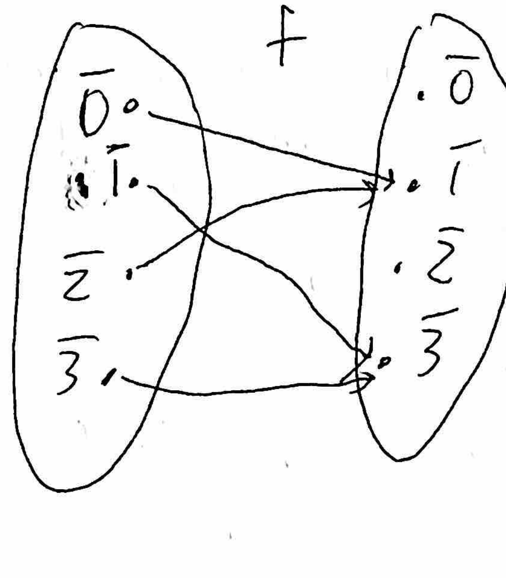
(i) f is not one-to-one since $f(1) = -15$ and $f(-1) = -15$ but $1 \neq -1$.

(ii) f is not onto $\mathbb{R}$, for example $-100 \in \mathbb{R}$ and if we try to solve $f(x) = -100$ or equivalently $x^4 - 16 = -100$ we get $x^4 = -84$. There does not exist $x \in \mathbb{R}$ with $x^4 = -84$ (you need complex numbers).

So, f is not onto $\mathbb{R}$.

(iii) f is not a bijection since f is not one-to-one and not onto.

2(e) $f: \mathbb{Z}_4 \to \mathbb{Z}_4$, $f(\bar{x}) = \bar{2}\bar{x} + \bar{1}$



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

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

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

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

(i) f is not one-to-one $f(\bar{0}) = f(\bar{2})$ and $\bar{0} \neq \bar{2}$

(ii) f is not onto. $\bar{0} \in \mathbb{Z}_4$ and there does not exist $\bar{x} \in \mathbb{Z}_4$ with $f(\bar{x}) = \bar{0}$

(iii) f is not a bijection

2(f) $f: M_2(\mathbb{R}) \to \mathbb{R}$ with $f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a+d$

(i) f is not one-to-one. For example,

$f\begin{pmatrix} 1 & 5 \\ -2 & -1 \end{pmatrix} = 1-1=0$ and $f\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0+0=0$

but $\begin{pmatrix} 1 & 5 \\ -2 & -1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(ii) f is onto. Given $y \in \mathbb{R}$, the matrix $\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ and $f\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} = y+0=y$.

(iii) f is not bijective since f is not 1-1.

2(g) $f: M_2(\mathbb{R}) \to \mathbb{R}$ with $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc$.

(i) f is not one-to-one since

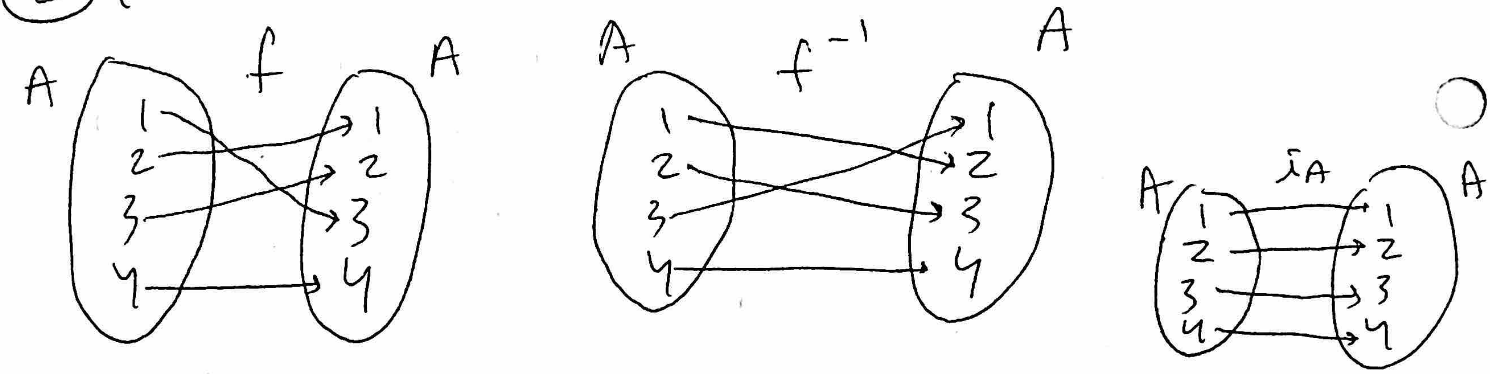
$f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ and $f\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = 1$

but $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

(ii) f is onto. Let $y \in \mathbb{R}$. Then $\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$ and $f\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = y$.

(iii) f is not bijective since f is not one-to-one.

3 (a)



$$\left.\begin{aligned}(f\circ f^{-1})(1)&=f(f^{-1}(1))=f(2)=1\\(f\circ f^{-1})(2)&=f(f^{-1}(2))=f(3)=2\\(f\circ f^{-1})(3)&=f(f^{-1}(3))=f(1)=3\\(f\circ f^{-1})(4)&=f(f^{-1}(4))=f(4)=4\end{aligned}\right\}\text{ So, } f\circ f^{-1}=i_A$$

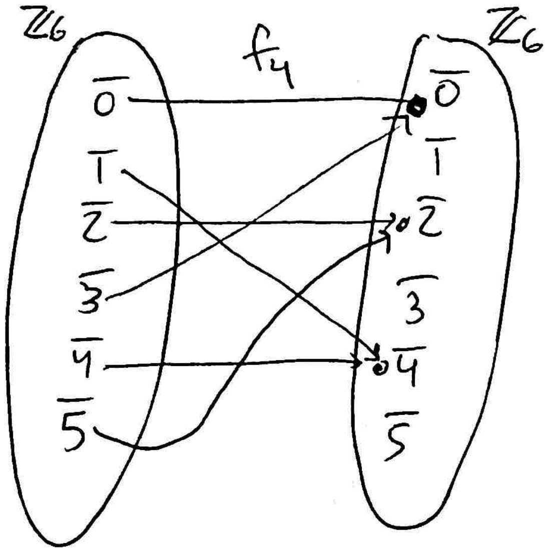
$$\left.\begin{aligned}(f^{-1}\circ f)(1)&=f^{-1}(f(1))=f^{-1}(3)=1\\(f^{-1}\circ f)(2)&=f^{-1}(f(2))=f^{-1}(1)=2\\(f^{-1}\circ f)(3)&=f^{-1}(f(3))=f^{-1}(2)=3\\(f^{-1}\circ f)(4)&=f^{-1}(f(4))=f^{-1}(4)=4\end{aligned}\right\}\text{ So, } f^{-1}\circ f=i_A$$

3 (b) You do (b). It's similar to (a).

4) (a) First note that given $\overline{x} \in \mathbb{Z}_n$, ie $x \in \mathbb{Z}$ we have that $\overline{a} \cdot \overline{x} = \overline{ax}$ is a valid element in $\mathbb{Z}_n$ since $ax \in \mathbb{Z}$,

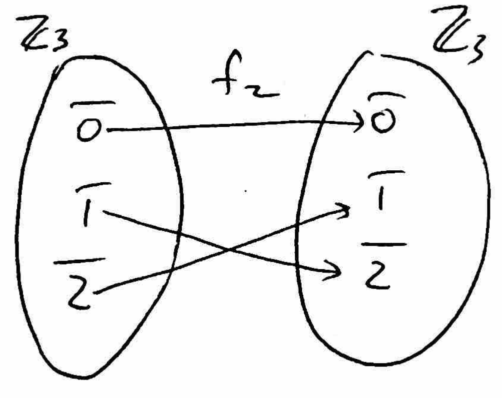
Now Suppose that $\overline{x} = \overline{y}$ where $\overline{x}, \overline{y} \in \mathbb{Z}_n$.
We need to show that $f_a(\overline{x}) = f_a(\overline{y})$.
In class we proved that since $\overline{x} = \overline{y}$ and $\overline{a} = \overline{a}$ we have that $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$.
Hence $f_a(\overline{x}) = f_a(\overline{y})$.

(b)



$f_4(\overline{0}) = \overline{4} \cdot \overline{0} = \overline{0}$
$f_4(\overline{1}) = \overline{4} \cdot \overline{1} = \overline{4}$
$f_4(\overline{2}) = \overline{4} \cdot \overline{2} = \overline{8} = \overline{2}$
$f_4(\overline{3}) = \overline{4} \cdot \overline{3} = \overline{12} = \overline{0}$
$f_4(\overline{4}) = \overline{4} \cdot \overline{4} = \overline{16} = \overline{4}$
$f_5(\overline{4}) = \overline{5} \cdot \overline{4} = \overline{20} = \overline{2}$

(c)



$f_2(\overline{0}) = \overline{2} \cdot \overline{0} = \overline{0}$
$f_2(\overline{1}) = \overline{2} \cdot \overline{1} = \overline{2}$
$f_2(\overline{2}) = \overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$

(d) Given $\overline{x} \in \mathbb{Z}_n$ we have that
$$(f_c \circ f_d)(\overline{x}) = f_c(f_d(\overline{x})) = f_c(\overline{d} \cdot \overline{x}) = \overline{c} \cdot (\overline{d} \cdot \overline{x})$$
$$= \overline{c} \cdot (\overline{dx}) = \overline{cdx} = \overline{cd} \cdot \overline{x} = f_{cd}(\overline{x}).$$

(e) Given $\bar{x} \in \mathbb{Z}_n$ we have that

$$f_{cd}(\bar{x}) = \overline{cd} \cdot \bar{x} = \overline{dc} \cdot \bar{x} = f_{dc}(\bar{x}).$$

(f) Suppose that $y \equiv w \pmod{n}$.

Then, from class, we know that $\bar{y} = \bar{w}$ in $\mathbb{Z}_n$.

~~Thus, from class, since $\bar{y} = \bar{w}$ and~~

Pick any $\bar{x} \in \mathbb{Z}_n$. From class we know that since $\bar{y} = \bar{w}$ and $\bar{x} = \bar{x}$ we have $\bar{y} \cdot \bar{x} = \bar{w} \cdot \bar{x}$,

So, $f_y(\bar{x}) = f_w(\bar{x})$,

Thus, $f_y = f_w$.

(g) Let $d = \gcd(a,n) > 1$.

Then $\underbrace{1 \leq \frac{n}{d} < n}_{\text{since } 1 < d \leq n}$ and $\frac{n}{d} \in \mathbb{Z}$ (since d divides n)

Thus, $\overline{\left(\frac{n}{d}\right)} \in \mathbb{Z}_n$ and $\overline{\left(\frac{n}{d}\right)} \neq \bar{0}$.

We have $f_a\left(\overline{\frac{n}{d}}\right) = \bar{a}\,\overline{\frac{n}{d}} = \overline{\left(a \cdot \frac{n}{d}\right)} = \overline{\left(\frac{a}{d} \cdot n\right)} =$

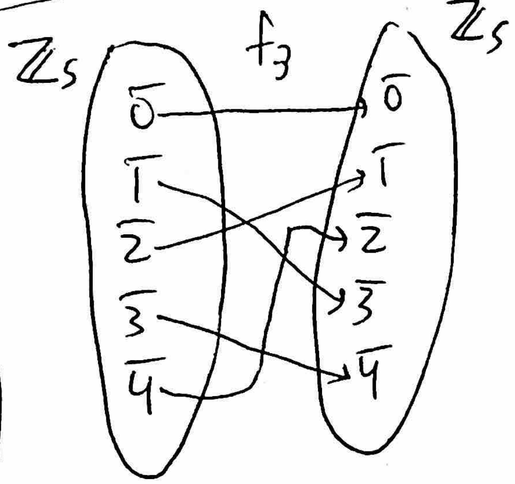
$= \overline{\left(\frac{a}{d}\right)} \cdot \bar{n} = \overline{\left(\frac{a}{d}\right)} \cdot \bar{0} = \bar{0}$

$\bar{n} = \bar{0}$ in $\mathbb{Z}_n$

d divides a since $d = \gcd(a,n)$. So, $\frac{a}{d} \in \mathbb{Z}$

So, $f_a(\bar{0}) = \bar{0} = f_a\left(\overline{\frac{n}{d}}\right)$ and $\bar{0} \neq \overline{\frac{n}{d}}$. Thus, f_a is not one-to-one if $\gcd(a,n) > 1$.

(h) Note that $f_3 : \mathbb{Z}_5 \to \mathbb{Z}_5$ is defined as $f_3(\bar{x}) = \bar{3} \cdot \bar{x}$. From the calculations, we see that f_3 is a bijection.

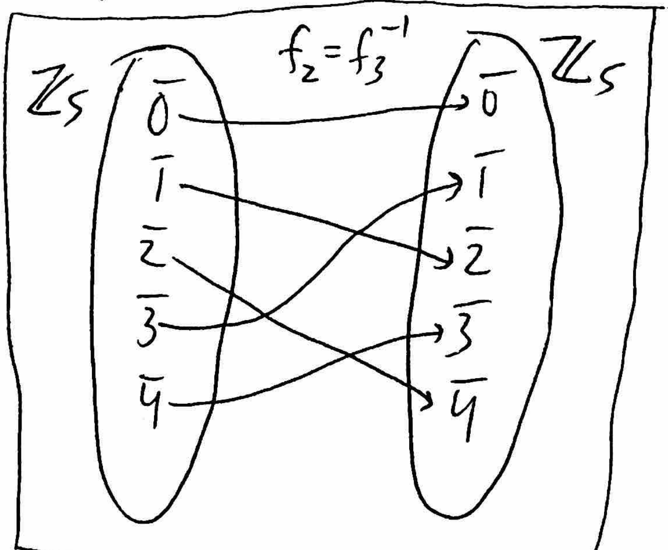


$f_3(\bar{0}) = \bar{3} \cdot \bar{0} = \bar{0}$
$f_3(\bar{1}) = \bar{3} \cdot \bar{1} = \bar{3}$
$f_3(\bar{2}) = \bar{3} \cdot \bar{2} = \bar{6} = \bar{1}$
$f_3(\bar{3}) = \bar{3} \cdot \bar{3} = \bar{9} = \bar{4}$
$f_4(\bar{4}) = \bar{3} \cdot \bar{4} = \overline{12} = \bar{2}$

To find f_3^{-1} we need to solve
$$\bar{y} = \bar{3} \cdot \bar{x}$$
for $\bar{x}$.

If we could find a $\bar{3}^{-1}$ element in $\mathbb{Z}_5$ we would be set. Note that $\bar{2} \cdot \bar{3} = \bar{1}$. So, $\bar{2}$ is like $\bar{3}^{-1}$. Given $\bar{y} = \bar{3} \cdot \bar{x}$ we multiply by $\bar{2}$ and get $\bar{2} \cdot \bar{y} = \bar{2} \cdot \bar{3} \cdot \bar{x}$ which gives $\bar{2} \cdot \bar{y} = \bar{x}$. That is, $f_3^{-1}(\bar{y}) = \bar{2}\bar{y}$

So, $f_3^{-1} = f_2$.

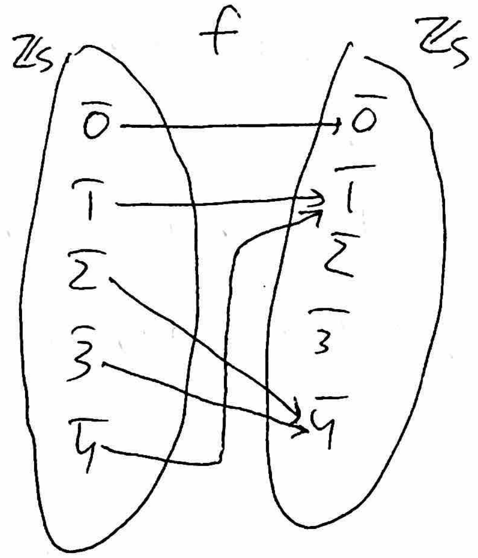


(5)

(a) First note that given $x \in \mathbb{Z}$ we have that $x^2 \in \mathbb{Z}$ and so $\overline{x^2} = \overline{x}^2$ is a valid element of $\mathbb{Z}_n$.

Suppose now that $\overline{a} = \overline{b}$ for some $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

From class we showed that we can multiply the equations $\overline{a} = \overline{b}$ and $\overline{a} = \overline{b}$ to get $\overline{a}^2 = \overline{b}^2$. Thus, $f(\overline{a}) = f(\overline{b})$ and f is well-defined.

(b) 

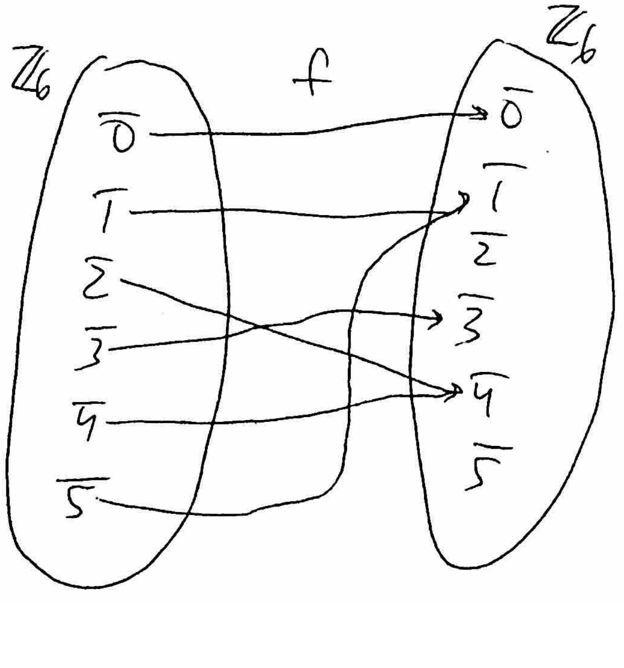
$f(\overline{0}) = \overline{0}^2 = \overline{0}$

$f(\overline{1}) = \overline{1}^2 = \overline{1}$

$f(\overline{2}) = \overline{2}^2 = \overline{4}$

$f(\overline{3}) = \overline{3}^2 = \overline{9} = \overline{4}$

$f(\overline{4}) = \overline{4}^2 = \overline{16} = \overline{1}$

(c) 

$f(\overline{0}) = \overline{0}^2 = \overline{0}$

$f(\overline{1}) = \overline{1}^2 = \overline{1}$

$f(\overline{2}) = \overline{2}^2 = \overline{4}$

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

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

$f(\overline{5}) = \overline{5}^2 = \overline{25} = \overline{1}$

(d) f is not one-to-one if $n>2$.
(Why?) Note that if $n>2$ then $1\not\equiv -1 \pmod n$ since if $1\equiv -1 \pmod n$ we would have that n divides $1-(-1)=2$ which would imply that $n=1$ or $n=2$. But $n>2$. Thus, $1\not\equiv -1 \pmod n$.

So, $\overline{1}\neq\overline{-1}$.

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

So, f is not one-to-one.

---

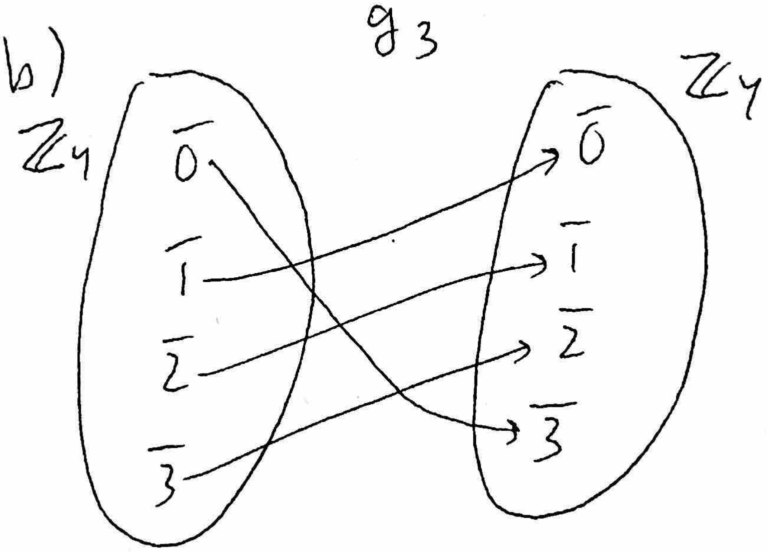
(6) f is not well-defined.
Note that $\frac{2}{1}=\frac{4}{2}$ but $f(\frac{2}{1})=2$ and $f(\frac{4}{2})=4$.

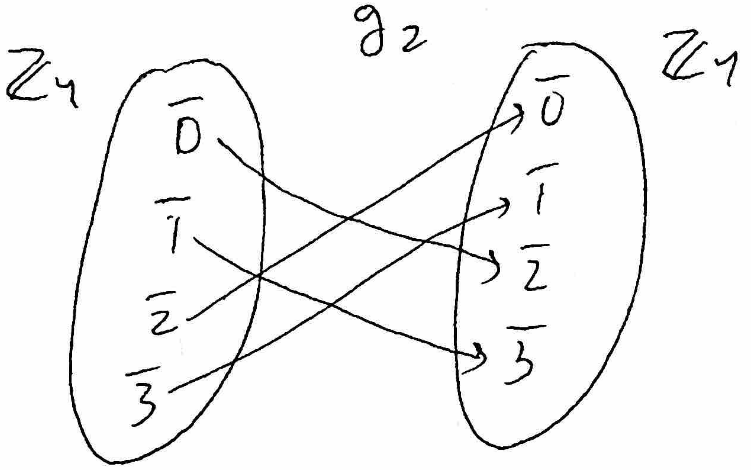
---

(7)

(a) Note that if $x\in\mathbb{Z}$ then $\overline{x}+\overline{a}=\overline{x+a}$ is a valid element of $\mathbb{Z}_n$ since $x+a\in\mathbb{Z}$.
Now suppose that $\overline{x},\overline{y}\in\mathbb{Z}_n$ with $\overline{x}=\overline{y}$.
We must show that $g_a(\overline{x})=g_a(\overline{y})$.
From class we know that since $\overline{x}=\overline{y}$ and $\overline{a}=\overline{a}$ we may add the equations to get $\overline{x}+\overline{a}=\overline{y}+\overline{a}$. Hence $g_a(\overline{x})=g_a(\overline{y})$.

(b)





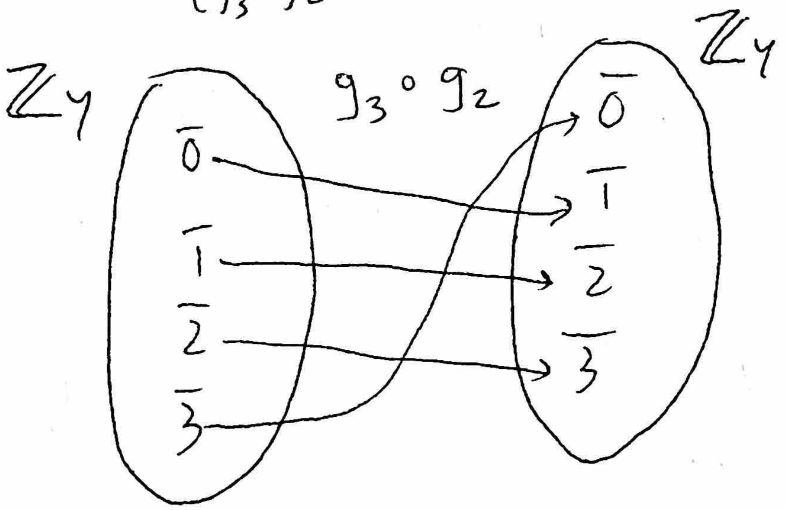
(c)

$(g_3 \circ g_2)(\bar{0}) = g_3(g_2(\bar{0})) = g_3(\bar{2}) = \bar{1}$

$(g_3 \circ g_2)(\bar{1}) = g_3(g_2(\bar{1})) = g_3(\bar{3}) = \bar{2}$

$(g_3 \circ g_2)(\bar{2}) = g_3(g_2(\bar{2})) = g_3(\bar{0}) = \bar{3}$

$(g_3 \circ g_2)(\bar{3}) = g_3(g_2(\bar{3})) = g_3(\bar{1}) = \bar{0}$



You do $g_2 \circ g_3$

You will get the same function as $g_3 \circ g_2$

(d) g_a is one-to-one

Suppose that $g_a(\overline{x}) = g_a(\overline{y})$ for some $\overline{x}, \overline{y} \in \mathbb{Z}_n$.

Then $\overline{x} + \overline{a} = \overline{y} + \overline{a}$.

So, $\overline{x} + \overline{a} + \overline{-a} = \overline{y} + \overline{a} + \overline{-a}$.

Thus, $\overline{x} + \overline{a-a} = \overline{y} + \overline{a-a}$.

So, $\overline{x} = \overline{y}$.

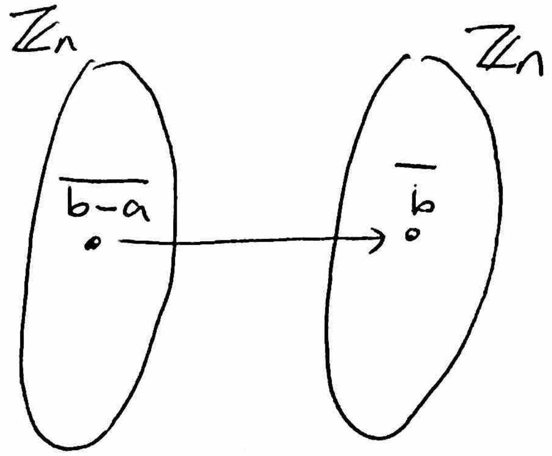
g_a is onto

Let $\overline{b} \in \mathbb{Z}_n$,

where $b \in \mathbb{Z}$.

Then $b - a \in \mathbb{Z}$

and so $\overline{b-a} \in \mathbb{Z}_n$.



And

$$g_a(\overline{b-a}) = \overline{b-a} + \overline{a}$$
$$= \overline{b} + \overline{-a} + \overline{a}$$
$$= \overline{b} + \overline{0} = \overline{b}$$

So, g_a is onto $\mathbb{Z}_n$

(e) From part d we get the formula $g_a^{-1}(\overline{x}) = \overline{x} + \overline{-a}$. We can verify this.

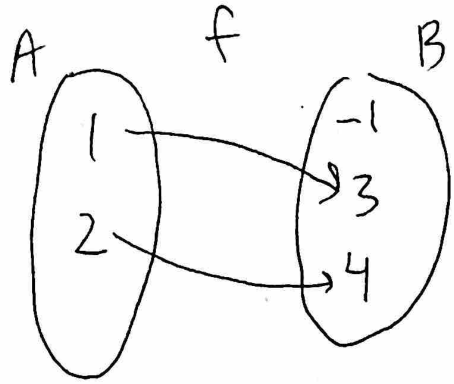
For any $\overline{x} \in \mathbb{Z}_n$ we have

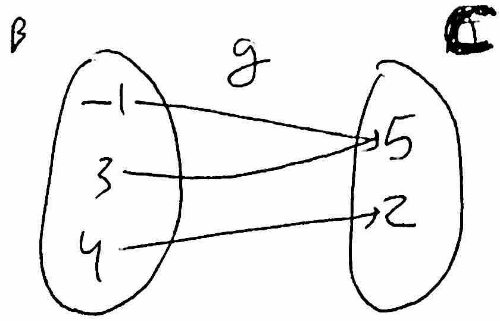
$g_a(g_a^{-1}(\overline{x})) = g_a(\overline{x} + \overline{-a}) = \overline{x} + \overline{-a} + \overline{a} = \overline{x} = i_{\mathbb{Z}_n}(\overline{x})$

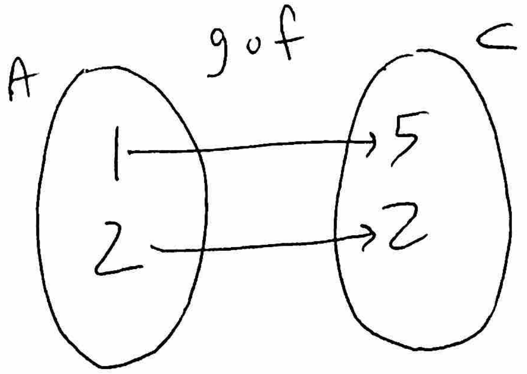
and $g_a^{-1}(g_a(\overline{x})) = g_a^{-1}(\overline{x} + \overline{a}) = \overline{x} + \overline{a} + \overline{-a} = \overline{x} = i_{\mathbb{Z}_n}(\overline{x})$.

So, $g_a \circ g_a^{-1} = i_{\mathbb{Z}_n}$ and $g_a^{-1} \circ g_a = i_{\mathbb{Z}_n}$ So in fact $g_a^{-1}(\overline{x}) = \overline{x} + \overline{-a}$.

8 (a)







f is not onto

$g \circ f$ is onto

(b) Use the same example as part (a). g is not one-to-one but $g \circ f$ is one-to-one

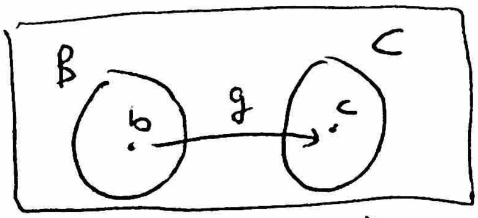
---

9 We have that f is not one-to-one. Thus there exist $a_1, a_2 \in A$ with $a_1 \neq a_2$ and $f(a_1) = f(a_2)$. Applying g to both sides we get $g(f(a_1)) = g(f(a_2))$. Hence $a_1 \neq a_2$ and $(g \circ f)(a_1) = (g \circ f)(a_2)$.

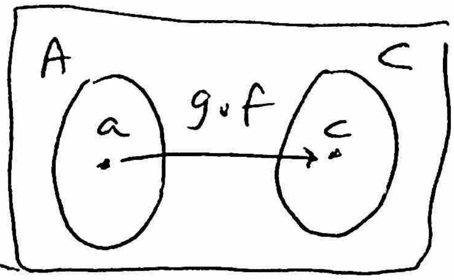
Thus, $g \circ f$ is not one-to-one.

(10) We prove the contrapositive:
"If $g \circ f$ is onto, then g is onto."

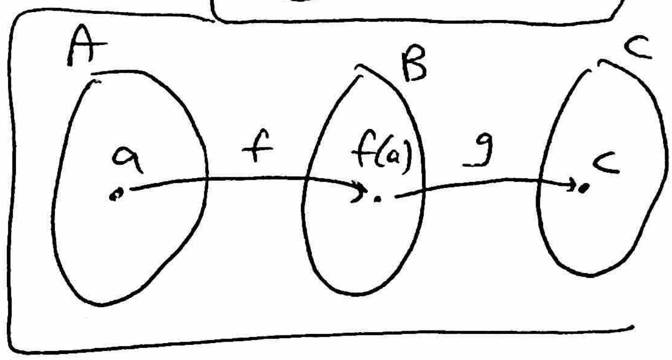
Assume that $g \circ f$ is onto.
Let's show that g is onto.
Let $c \in C$.
We need to find $b \in B$ with $g(b) = c$. Ie this picture.



Since $g \circ f$ is onto and $g \circ f : A \to C$ there exists $a \in A$ with $(g \circ f)(a) = c$.

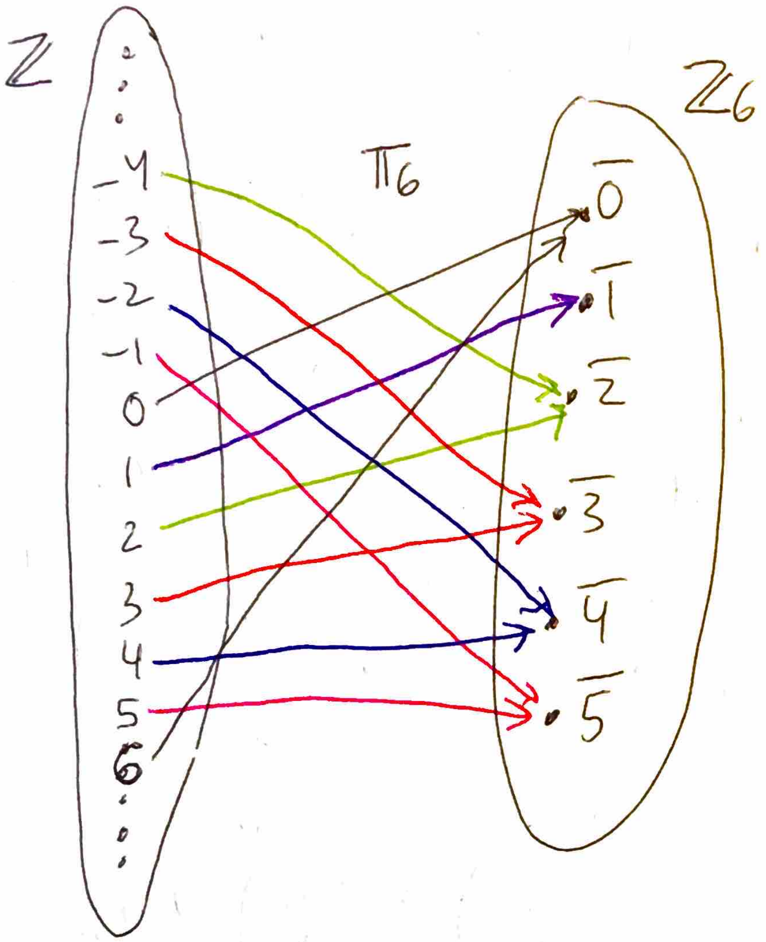


Unravelling this we have $g(f(a)) = c$ and $f(a) \in B$.



So, set $b = f(a)$.
Then,
$$g(b) = g(f(a)) = c.$$
So, g is onto.

11 (a)



$\pi_6(-1) = \overline{-1} = \overline{5}$

$\pi_6(10) = \overline{10} = \overline{4}$

$\pi_6(7) = \overline{7} = \overline{1}$

$\pi_6(-17) = \overline{-17} = \overline{1}$

π_6 is not one-to-one.

π_6 is onto $\mathbb{Z}_6$.

(b) $\pi_6(X) = \{\pi_6(1), \pi_6(17), \pi_6(-5), \pi_6(102), \pi_6(-13)\}$

$= \{\overline{1}, \overline{17}, \overline{-5}, \overline{102}, \overline{-13}\}$

$= \{\overline{1}, \overline{5}, \overline{1}, \overline{0}, \overline{5}\} = \{\overline{0}, \overline{1}, \overline{5}\}$

(c) $\pi_6^{-1}(\{\overline{0}\}) = \{6k \mid k \in \mathbb{Z}\}$.

$\boxed{\text{proof:}}$

$\boxed{\subseteq}$: Let $x \in \pi_6^{-1}(\{\overline{0}\})$. Then $\pi_6(x) \in \{\overline{0}\}$. So, $\pi_6(x) = \overline{0}$. Thus, $\overline{x} = \overline{0}$ in $\mathbb{Z}_6$. So, $x \equiv 0 \pmod 6$. Thus, $6 \mid (x-0)$. So, $6 \mid x$. Thus, $x = 6k$ for some $k \in \mathbb{Z}$.
Thus, $x \in \{6k \mid k \in \mathbb{Z}\}$.

$\boxed{\supseteq}$: Now suppose $x \in \{6k \mid k \in \mathbb{Z}\}$.
Then $x = 6k$ where $k \in \mathbb{Z}$.
We have $\pi_6(x) = \overline{x} = \overline{6k} = \overline{6}\,\overline{k} = \overline{0}\,\overline{k} = \overline{0}$ in $\mathbb{Z}_6$.
Thus, $x \in \pi_6^{-1}(\{\overline{0}\})$.

By $\boxed{\subseteq}$ and $\boxed{\supseteq}$ we have $\pi_6^{-1}(\{\overline{0}\}) = \{6k \mid k \in \mathbb{Z}\}$.

(d) $\pi_6^{-1}(\{\overline{1}\}) = \{6k+1 \mid k \in \mathbb{Z}\}$.

proof:
Let's prove this differently than part c. You could do a similar proof to c if you like.
We have that

$$\begin{aligned}
\pi_6^{-1}(\{\overline{1}\}) &= \{x \in \mathbb{Z} \mid \pi_6(x) \in \{\overline{1}\}\} \\
&= \{x \in \mathbb{Z} \mid \pi_6(x) = \overline{1}\} \\
&= \{x \in \mathbb{Z} \mid \overline{x} = \overline{1} \text{ in } \mathbb{Z}_6\} \\
&= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{6}\} \\
&= \{x \in \mathbb{Z} \mid 6 \mid (x-1)\} \\
&= \{x \in \mathbb{Z} \mid x-1 = 6k \text{ for some } k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \mid x = 6k+1 \text{ for some } k \in \mathbb{Z}\} \\
&= \{6k+1 \mid k \in \mathbb{Z}\}.
\end{aligned}$$

(e) $\pi_6^{-1}(\{\bar{0},\bar{3}\}) = \{x \in \mathbb{Z} \mid \pi_6(x) \in \{\bar{0},\bar{3}\}\}$

$= \{x \in \mathbb{Z} \mid \pi_6(x) = \bar{0} \text{ or } \pi_6(x) = \bar{3}\}$

$= \{x \in \mathbb{Z} \mid \bar{x} = \bar{0} \text{ or } x = \bar{3} \text{ in } \mathbb{Z}_6\}$

$= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 6 \text{ or } x \equiv 3 \pmod 6\}$

If $x \equiv 3 \pmod 6$ then $6 \mid (x-3)$, so $x-3 = 6\ell$ for some $\ell \in \mathbb{Z}$

$= \{x \in \mathbb{Z} \mid x = 6k \text{ for some } k \in \mathbb{Z} \text{ or } x = 6\ell + 3 \text{ for some } \ell \in \mathbb{Z}\}$

$= \{6k \mid k \in \mathbb{Z}\} \cup \{6\ell + 3 \mid \ell \in \mathbb{Z}\}$

---

(12) $f : A \times A \to A$ where $A = \mathbb{N} \cup \{0\}$
and $f(m,n) = m^2 + n^2$

(a) $f(3,5) = 3^2 + 5^2 = 9 + 25 = 34$
$f(1,1) = 1^2 + 1^2 = 2$
$f(2,1) = 2^2 + 1^2 = 5$

(b) $f(C) = \{f(0,0), f(1,10), f(2,5)\}$
$= \{0, 1^2 + 10^2, 2^2 + 5^2\} = \{0, 101, 29\}$

(c) Note that $\boxed{(m,n) \in f^{-1}(B)}$

iff $\boxed{f(m,n) \in B = \{1,2,3,4\}}$

iff $\boxed{f(m,n) = 1 \text{ or } f(m,n) = 2 \text{ or } f(m,n) = 3 \text{ or } f(m,n) = 4}$

iff $\boxed{m^2+n^2 = 1 \text{ or } m^2+n^2 = 2 \text{ or } m^2+n^2 = 3 \text{ or } m^2+n^2 = 4.}$

Case 1: The solutions to $m^2+n^2=1$ are $(m,n) = (1,0), (-1,0), (0,1), (0,-1)$

Case 2: The solutions to $m^2+n^2=2$ are $(m,n) = (1,1), (-1,1), (-1,-1), (1,-1)$

Case 3: There are no solutions to $m^2+n^2=3$ where $m,n \in A = \mathbb{N} \cup \{0\} = \{0,1,2,3,\ldots\}$

** * see part (e) for an explanation of this case * * **

Case 4: The solutions to $m^2+n^2=4$ are $(m,n) = (2,0), (-2,0), (0,2), (0,-2)$.

Hence, $f^{-1}(B) = \{(1,0), (-1,0), (0,1), (0,-1), (2,0), (-2,0), (0,2), (0,-2), (1,1), (1,-1), (-1,1), (-1,-1)\}$

(d) f is not one-to-one. For example $f(1,0) = f(-1,0)$ but $(1,0) \neq (-1,0)$

(e) f is not onto.

For example $3 \in A$ but there are no $(m,n) \in A \times A$ with $f(m,n) = 3$ since $m^2 + n^2 = 3$ has no solutions. You can see this by enumerating the first few cases:

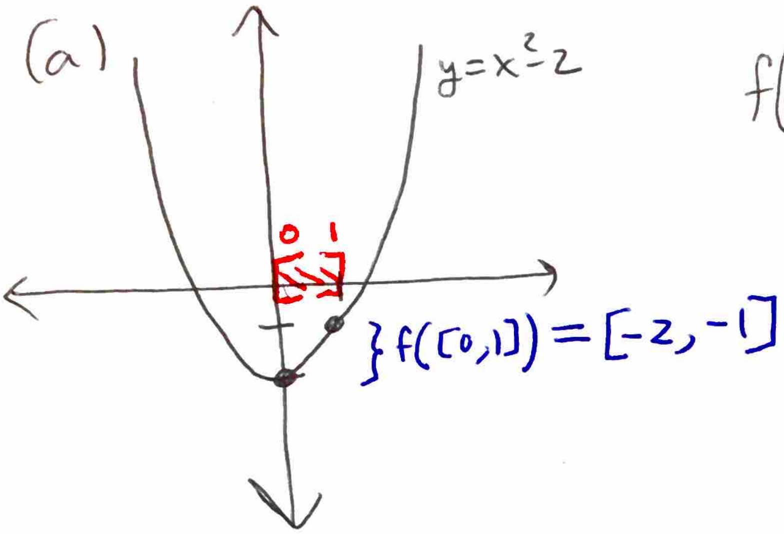
(m,n)	m^2+n^2
$(0,0)$	0
$(\pm 1, 0)$	1
$(0, \pm 1)$	1
$(\pm 1, \pm 1)$	2
$(0, \pm 2)$	4
$(\pm 2, 0)$	4
$(\pm 2, \pm 1)$	5
$\vdots$	$\vdots$

all other outputs are greater than 3

Thus f is not onto.

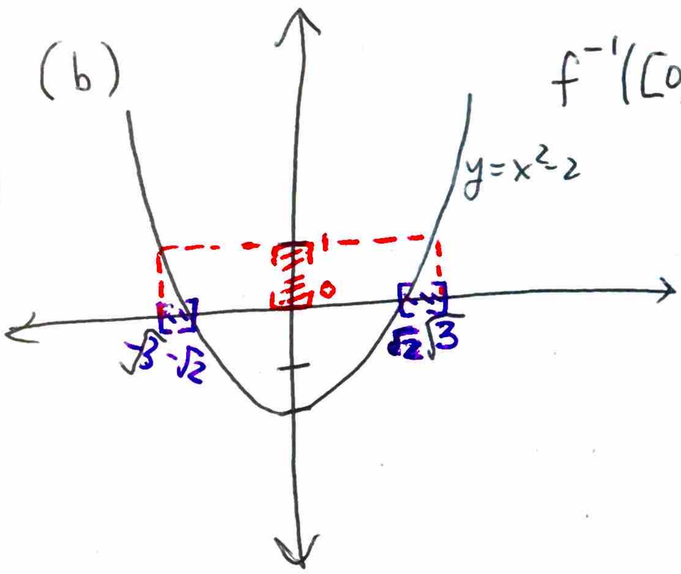
(13) $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - 2$

(a)



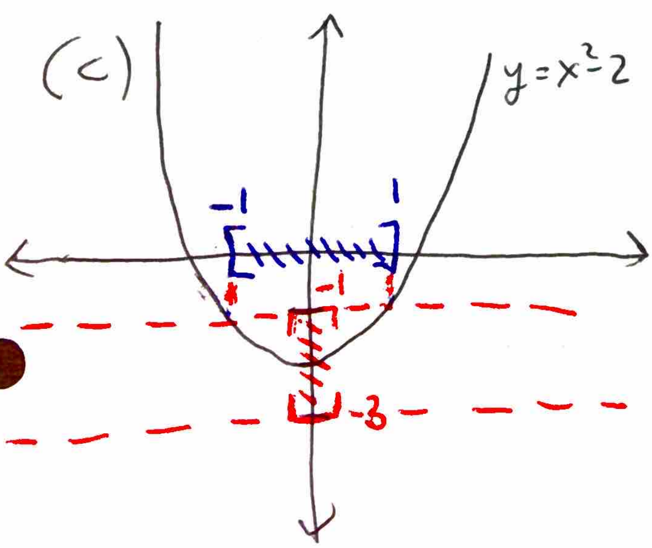
$$f([0,1]) = \{ f(x) \mid x \in [0,1] \}$$
$$= \{ x^2 - 2 \mid 0 \le x \le 1 \}$$
$$= [-2,-1]$$

(b)



$$f^{-1}([0,1]) = \{ x \mid f(x) \in [0,1] \}$$
$$= \{ x \mid 0 \le x^2 - 2 \le 1 \}$$
$$= [-\sqrt{3}, -\sqrt{2}] \cup [\sqrt{2}, \sqrt{3}]$$

(c)



$$f^{-1}([-3,-1]) = \{ x \mid f(x) \in [-3,-1] \}$$
$$= \{ x \mid -3 \le x^2 - 2 \le -1 \}$$
$$= [-1, 1]$$

(14)

(a) $f: X \to Y$, $W \subseteq X$, $Z \subseteq X$.

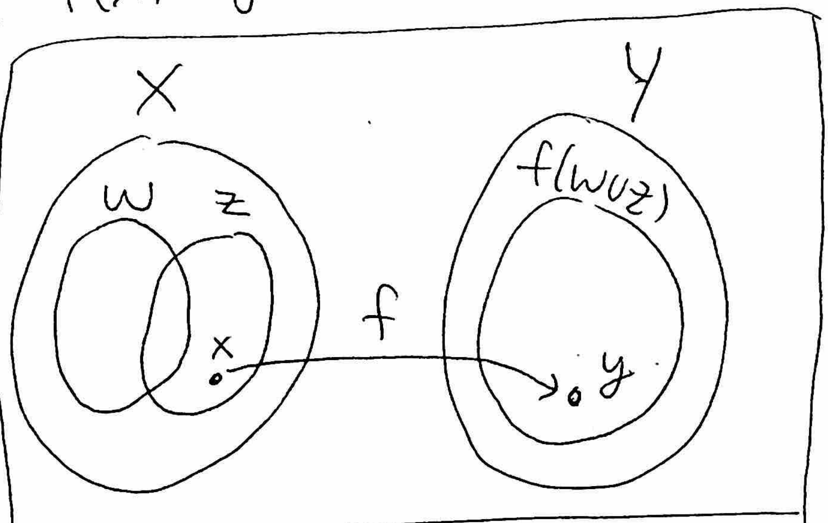
Prove: $f(W \cup Z) = f(W) \cup f(Z)$.

pf:

$(\subseteq)$: Let $y \in f(W \cup Z)$.

By definition this means that there exists $x \in W \cup Z$ with $f(x) = y$.

Since $x \in W \cup Z$ we have that $x \in W$ or $x \in Z$.



Picture where $x \in Z$

case 1: Suppose $x \in W$.

Then $y = f(x) \in f(W)$.

case 2: Suppose $x \in Z$.

Then $y = f(x) \in f(Z)$.

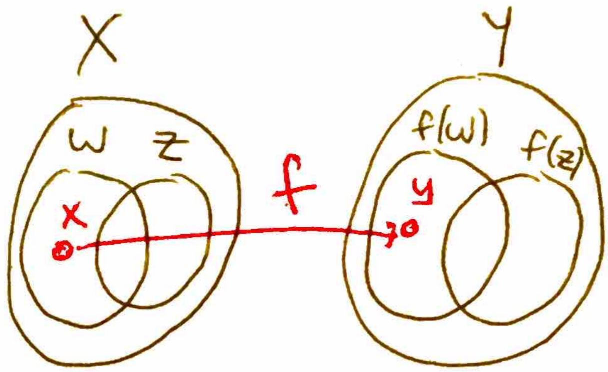
In either case, $y = f(x) \in f(W) \cup f(Z)$.

So, $f(W \cup Z) \subseteq f(W) \cup f(Z)$.

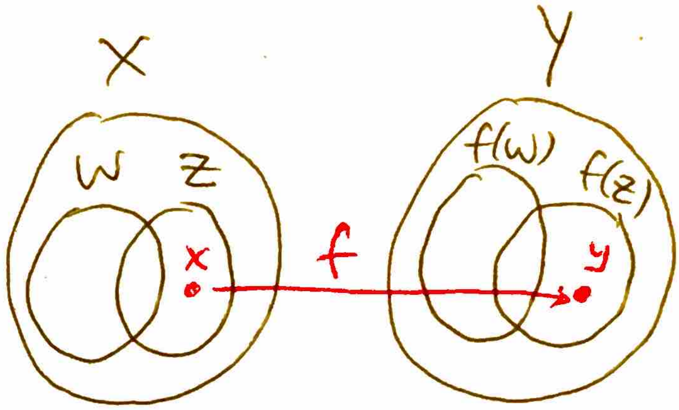
$\boxed{\supseteq}$: Let $y \in f(W) \cup f(Z)$.

Then $y \in f(W)$ or $y \in f(Z)$.

Case 1: Suppose $y \in f(W)$.
Then there exists $x \in W$ with $f(x) = y$.
Since $x \in W$ we have that $x \in W \cup Z$.
Thus, since $x \in W \cup Z$ and $f(x) = y$ we have that $y \in f(W \cup Z)$.



Case 2: Suppose $y \in f(Z)$.
Then there exists $x \in Z$ with $f(x) = y$.
Since $x \in Z$ we have that $x \in W \cup Z$.
Thus, since $x \in W \cup Z$ and $f(x) = y$ we have that $y \in f(W \cup Z)$.



In both cases, we get that $y \in f(W \cup Z)$.
Thus, $f(W) \cup f(Z) \subseteq f(W \cup Z)$.

By $\boxed{\subseteq}$ and $\boxed{\supseteq}$ we get that
$f(W) \cup f(Z) = f(W \cup Z)$. ▨

(14) (b) $f: X \to Y$, $A \subseteq Y$, $B \subseteq Y$.

Prove: $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

proof:

$\boxed{\subseteq}$: Let $x \in f^{-1}(A \cap B)$.

Then by definition $f(x) \in A \cap B$.

So, $f(x) \in A$ and $f(x) \in B$.

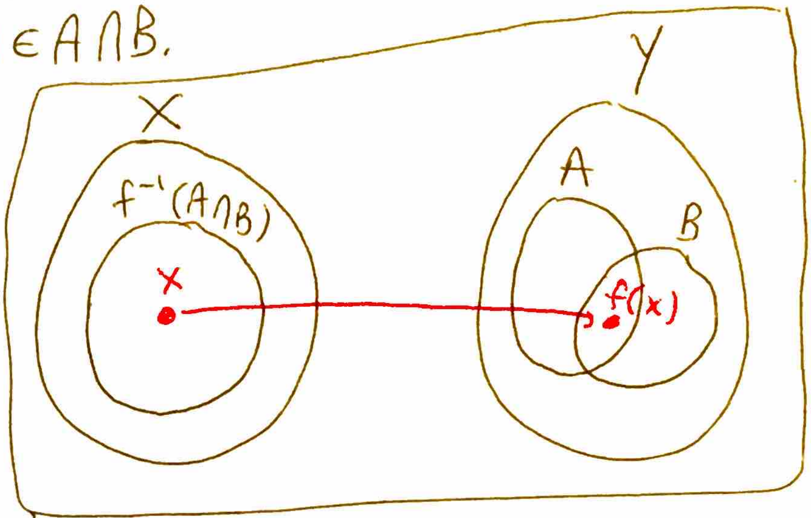
Thus, by definition,

$x \in f^{-1}(A)$ and $x \in f^{-1}(B)$.

So, $x \in f^{-1}(A) \cap f^{-1}(B)$.

Thus,

$f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.



$\boxed{\supseteq}$: Let $x \in f^{-1}(A) \cap f^{-1}(B)$.

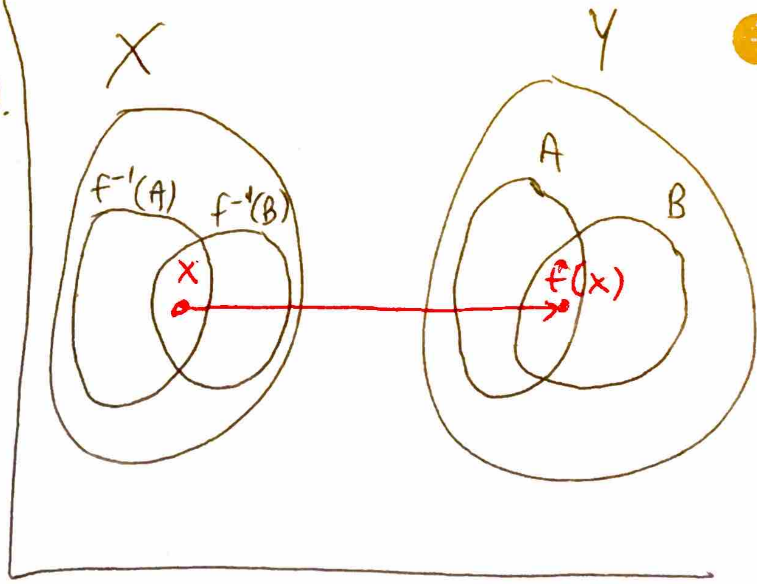
Then $x \in f^{-1}(A)$ and $x \in f^{-1}(B)$.

By definition, this means that $f(x) \in A$ and $f(x) \in B$.

So, $f(x) \in A \cap B$.

By def., this means that $x \in f^{-1}(A \cap B)$.

So, $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

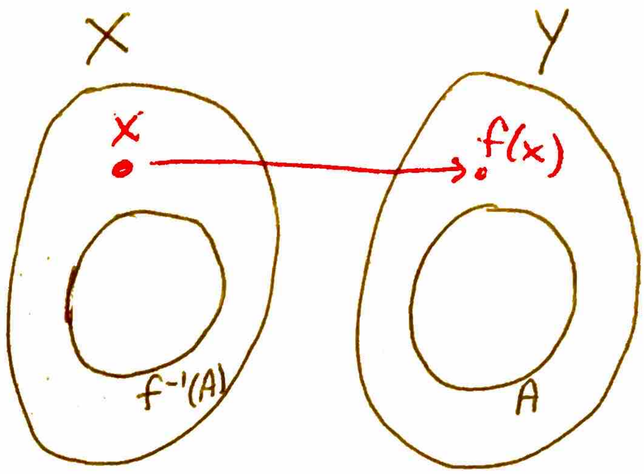


By $\boxed{\subseteq}$ and $\boxed{\supseteq}$ we get that

$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. $\boxtimes$

(14) (c) $f: X \to Y$; $A \subseteq Y$.

Prove: $X - f^{-1}(A) \subseteq f^{-1}(Y-A)$.



proof:

Let $x \in X - f^{-1}(A)$.

Then $x \in X$ and $x \notin f^{-1}(A)$.

So, $x \in X$ and $f(x) \notin A$.

Thus, $x \in X$ and $f(x) \in Y - A$.

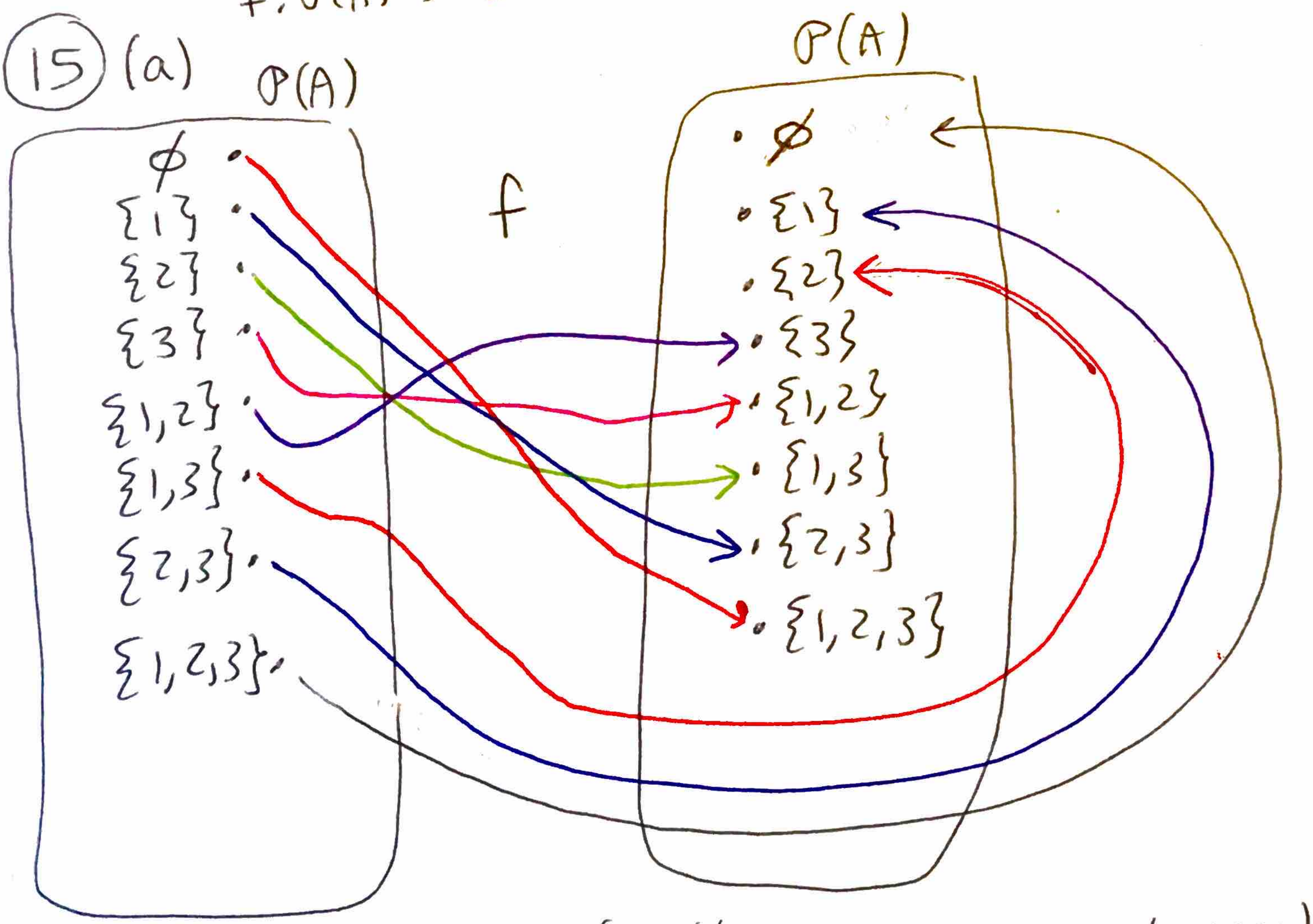
~~Therefore, $x \in X$ and~~

Therefore, $x \in f^{-1}(Y-A)$. ▨

So, $X - f^{-1}(A) \subseteq f^{-1}(Y-A)$

$f: \mathcal{P}(A) \to \mathcal{P}(A)$ where $f(X) = A - X$

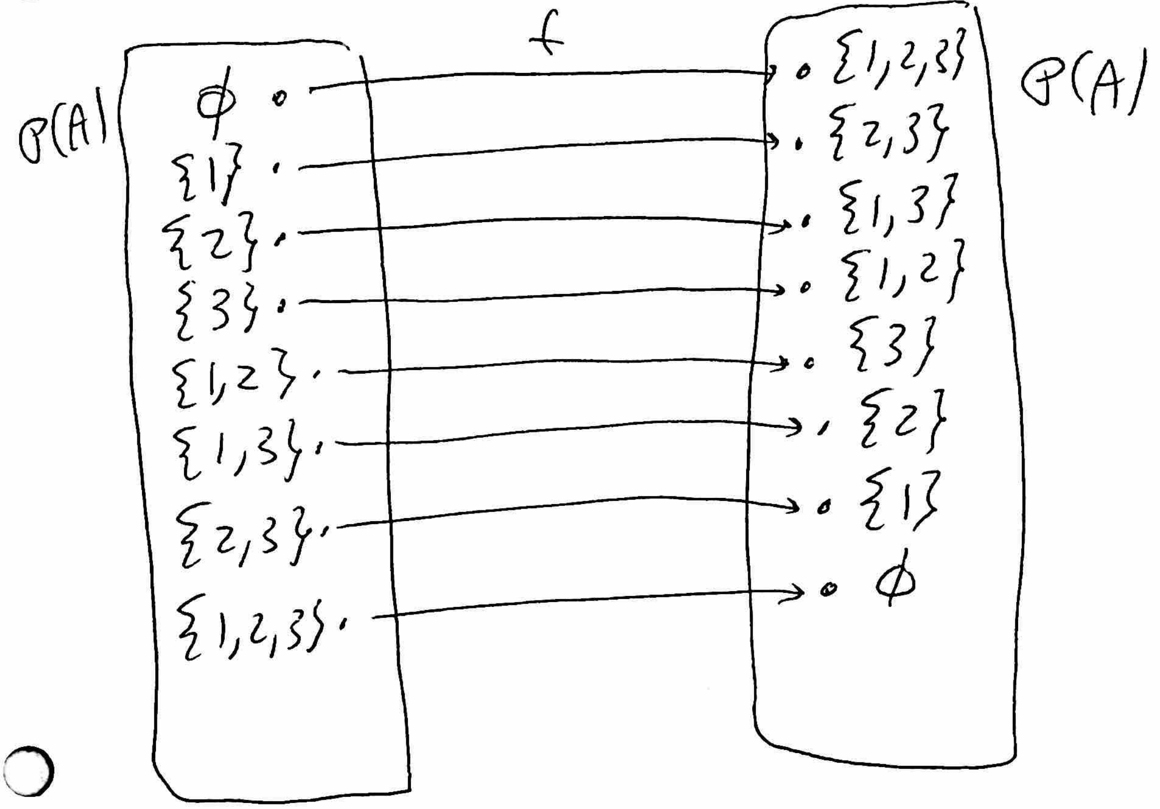
(15) (a)



(better picture on next page)

↓

If we just rearrange the elements on the right side of the picture then the function is easier to see.



(b) If $X \subseteq A$, then $A-(A-X)=X$.

pf: $\boxed{\subseteq}$: Let $a \in A-(A-X)$.

Then $a \in A$ and $a \notin A-X$.

So $a \in A$ and its not true that "$a \notin X$".

So, $a \in A$ and $a \in X$.

Thus, $a \in X$

So, $A-(A-X) \subseteq X$.

$\boxed{\supseteq}$: Let $x \in X \subseteq A$.

Then $x \in A$ and its not true that "$x \notin X$".

So, $x \in A$ and $x \notin A-X$.

Thus, $x \in A-(A-X)$.

So, $X \subseteq A-(A-X)$.

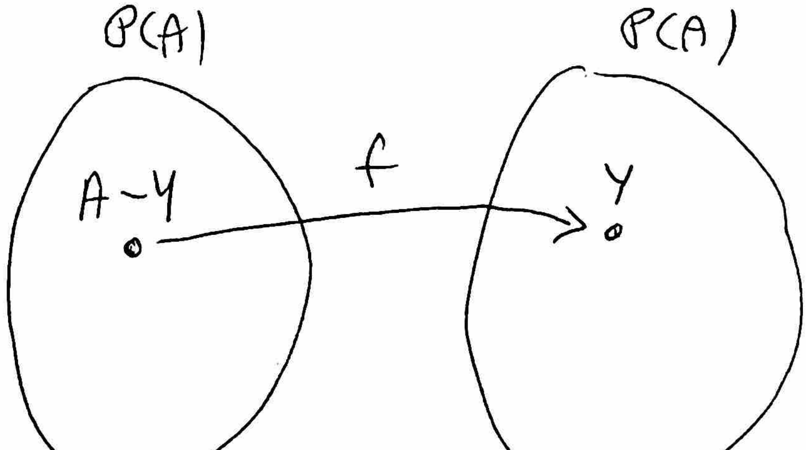
By $\boxed{\subseteq}$ and $\boxed{\supseteq}$ we have that $A-(A-X)=X$. $\blacksquare$

(c) In general, $f: \mathcal{P}(A) \to \mathcal{P}(A)$ given by $f(X) = A - X$ is a bijection.

pf:

(1-1) Suppose $f(X_1) = f(X_2)$ where $X_1, X_2 \in \mathcal{P}(A)$.
Then $A - X_1 = A - X_2$ and $X_1, X_2 \subseteq A$.
So, $A - (A - X_1) = A - (A - X_2)$.
By part (b) we get $X_1 = X_2$.
So, f is one-to-one.

(onto).
Let $Y \in \mathcal{P}(A)$.
That is, $Y \subseteq A$.
We need to find $X \in \mathcal{P}(A)$ with $f(X) = Y$.
Set $X = A - Y$.
Then, $f(X) = f(A - Y) = A - (A - Y) \overset{\text{part (b)}}{=} Y$.
So, f is onto.



By the above f is a bijection. ∎

(d) We can show that $f = f^{-1}$ by showing that $f \circ f = i$ where i is the identity function on $\mathcal{P}(A)$.

pf: Let $X \in \mathcal{P}(A)$.

Then

$$(f \circ f)(X) = f(f(X))$$
$$= f(A - X)$$
$$= A - (A - X) = X = i(X).$$

part(b)

$\blacksquare$