Lecture 7: Functions

Ashish Dandekar

AY2025/26 Semester 1

Part of the contents here is taken from Dr Wong Tin Lok's lecture notes.

Functions in C programming:

```
int f(int x, double y) {
    return x * sqrt(y);
}
```

$f(3, 4) \rightarrow 6.0$

$f(4, 3) \rightarrow 6.928203$

$f(6, 1) \rightarrow 6.0$

Many built-in math functions in C:

- floor(), round()
- ceil(), floor()
- sin(), cos(), tan()
- log(), log10()
- sqrt(), pow()
- etc.

Applications of function in Computer Science: computational complexity of algorithms, counting objects, study of sequences and strings, etc.

7.1 Definitions

- Definitions of function, arrow diagram, image, pre-image, setwise image, setwise preimage, domain, co-domain, range.
- Sequences, strings.
- Function equality.

7.2 Injections, Surjections, Bijections and Inverse Functions

- Injections, surjections, bijections.
- Inverse functions.
- Bijectivity and invertibility.

7.3 Composition of Functions

- Composition with the identity function; composition with its inverse.
- Associativity and noncommutativity of function composition.
- Composition of injections; composition of bijections.

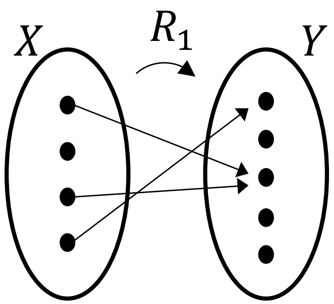
7.4 Addition and Multiplication on $\mathbb{Z}_n$

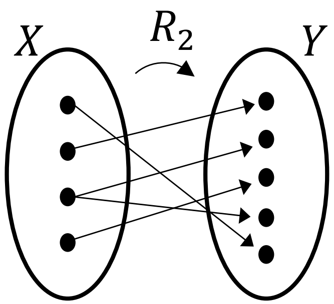
Reference: Epp's Chapter 7 Functions

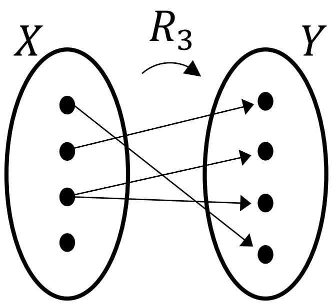
Recapitulation

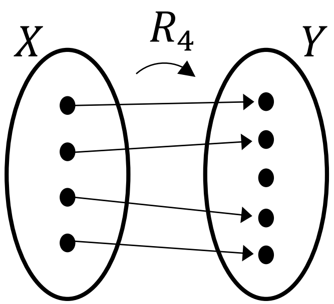
Definition: Relation

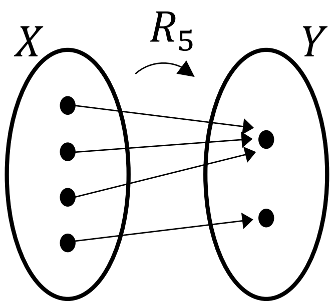
Let X and Y be sets. A (binary) **relation from $\boldsymbol{X}$ to $\boldsymbol{Y}$** is a subset of $\boldsymbol{X \times Y}$.
Given an ordered pair (x, y) in $X \times Y$, **$\boldsymbol{x}$ is related to $\boldsymbol{y}$ by $\boldsymbol{R}$**, or
$\boldsymbol{x}$ is $\boldsymbol{R}$-related to $\boldsymbol{y}$, written $\boldsymbol{x\ R\ y}$, iff $(\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{R}$.

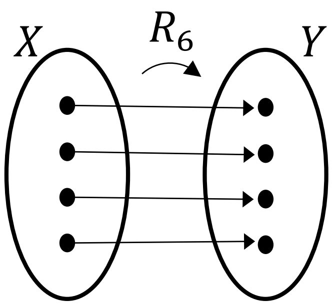












Recapitulation

Reflexive Property

Symmetric Property

Anti-symmetric Property

Transitive Property

(Not) symmetric Property

7.1 Definitions

7.1.1 Definitions

Definition: Function

A function f from a set X to a set Y, denoted $f: X \to Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X\ \exists y \in Y\ (x, y) \in f$.

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y\ \Big(\big((x, y_1) \in f \wedge (x, y_2) \in f\big) \to y_1 = y_2\Big)$.

(That is, the y in (F1) is unique.)

Or alternatively,

Let f be a relation on sets X and Y, i.e. $f \subseteq X \times Y$. Then f is a function from X to Y, denoted $f: X \to Y$, iff

$$\forall x \in X\ \exists!\, y \in Y\ (x, y) \in f.$$

Informally,

A function from X to Y is an assignment to each element of X exactly one element of Y.

Example #1: A function $f: \mathbb{R} \to \mathbb{R}$ is defined as follows: $\forall x \in \mathbb{R}$, $f(x)$ is the real number y such that $x^2 + y^2 = 1$.

Is the above a function? No!

Two reasons. For almost all values of x, either (1) there is no y that satisfies the given equation (eg: when $x = 2$), or (2) there are two different values of y that satisfy the equation (eg: when $x = 0$).

Definitions: Arrow Diagrams

If X and Y are finite sets, you can define a function f from X to Y by drawing an arrow diagram.

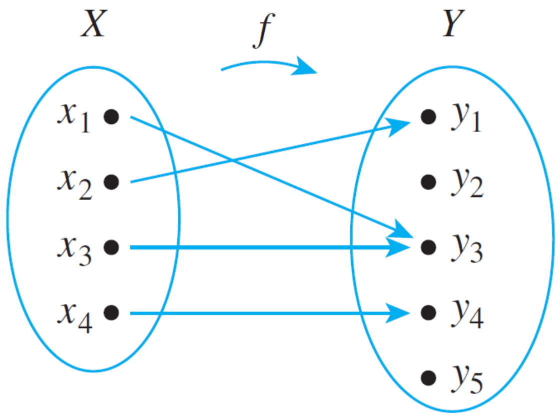


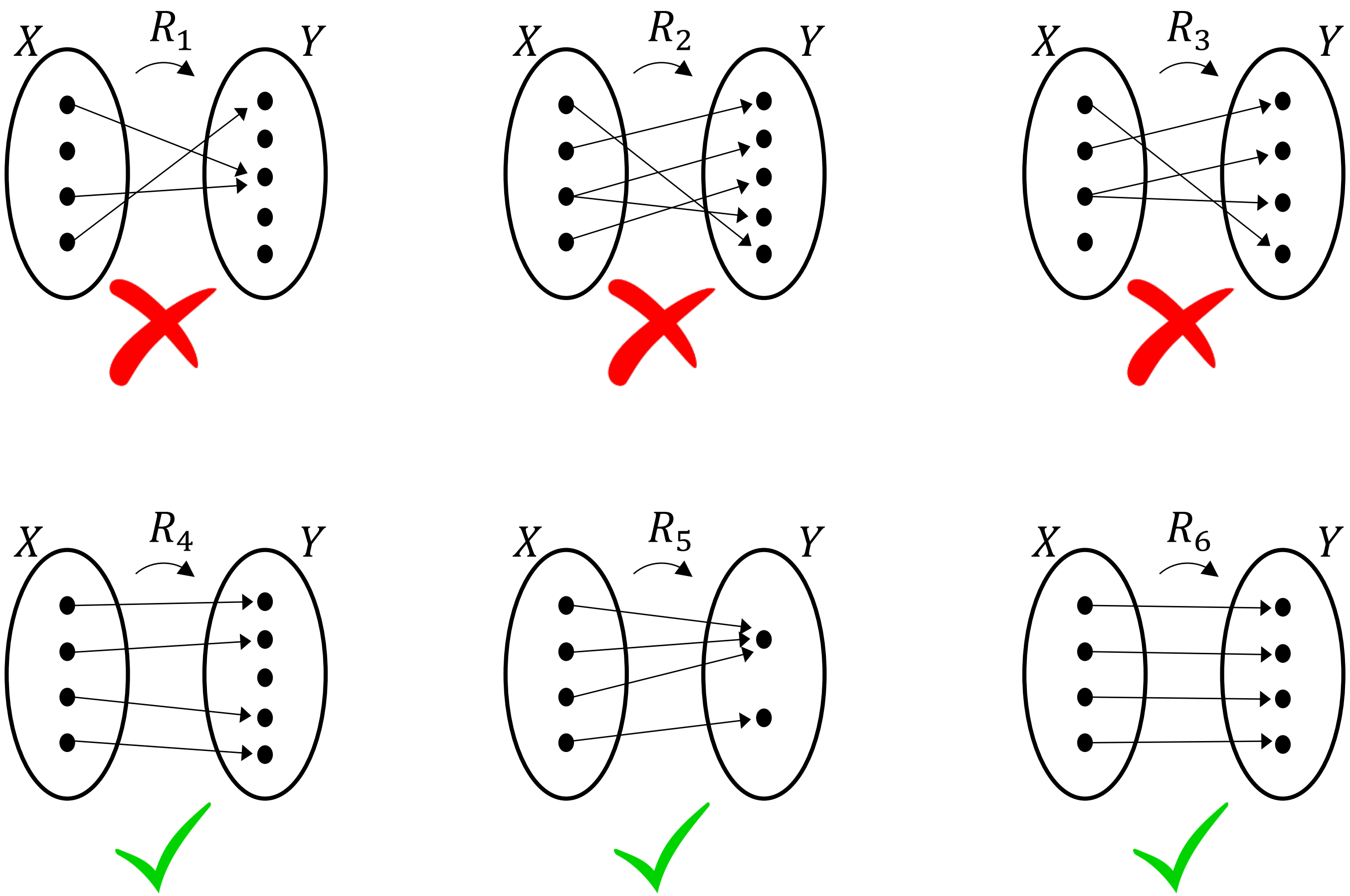
Figure 7.1.1

This arrow diagram defines a function because

1. Every element of X has an arrow coming out of it.
2. No element of X has two arrows coming out of it that point to two different elements of Y.

f is a function from X to Y, denoted $f: X \to Y$, iff
$\forall x \in X, \exists! y \in Y$ such that $(x, y) \in f$.

Example #2: Which of the following relations are functions and which are not? Why?



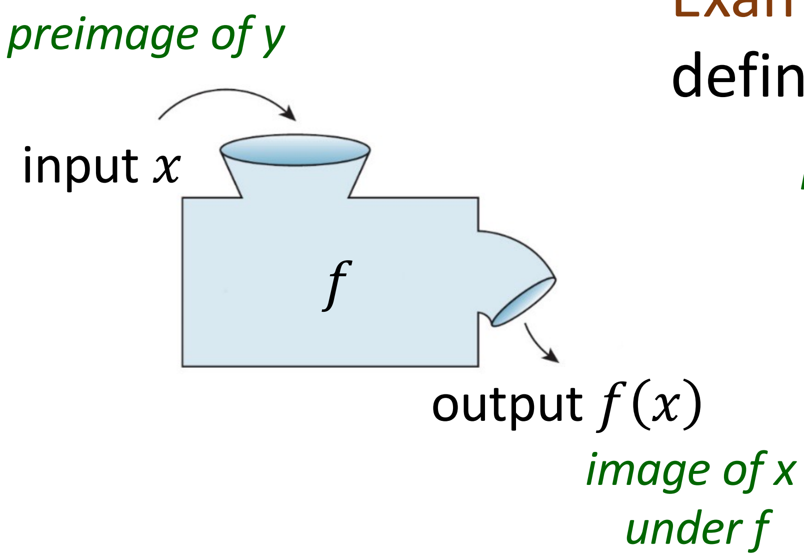
Definitions: Argument, image, preimage , input, output

Let $f: X \to Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$.

We say that "f sends/maps x to y" and we may also write $x \xrightarrow{f} y$ or $f: x \longmapsto y$. Also, x is called the **argument** of f.

$f(x)$ is read "f of x", or "the **output** of f for the **input** x", or "the value of f at x", or "the **image** of x under f".

If $f(x) = y$, then x is a **preimage** of y.



Example #3: A function $f: \mathbb{Z} \to \mathbb{Z}$ is defined as: $\forall x \in \mathbb{Z}, f(x) = 2x + 1$.

preimage x	$f(x)$ *image*
0	1
1	3
7	15
-5	-9

Definitions: Setwise image and preimage

Let $f : X \to Y$ be a function from set X to set Y.

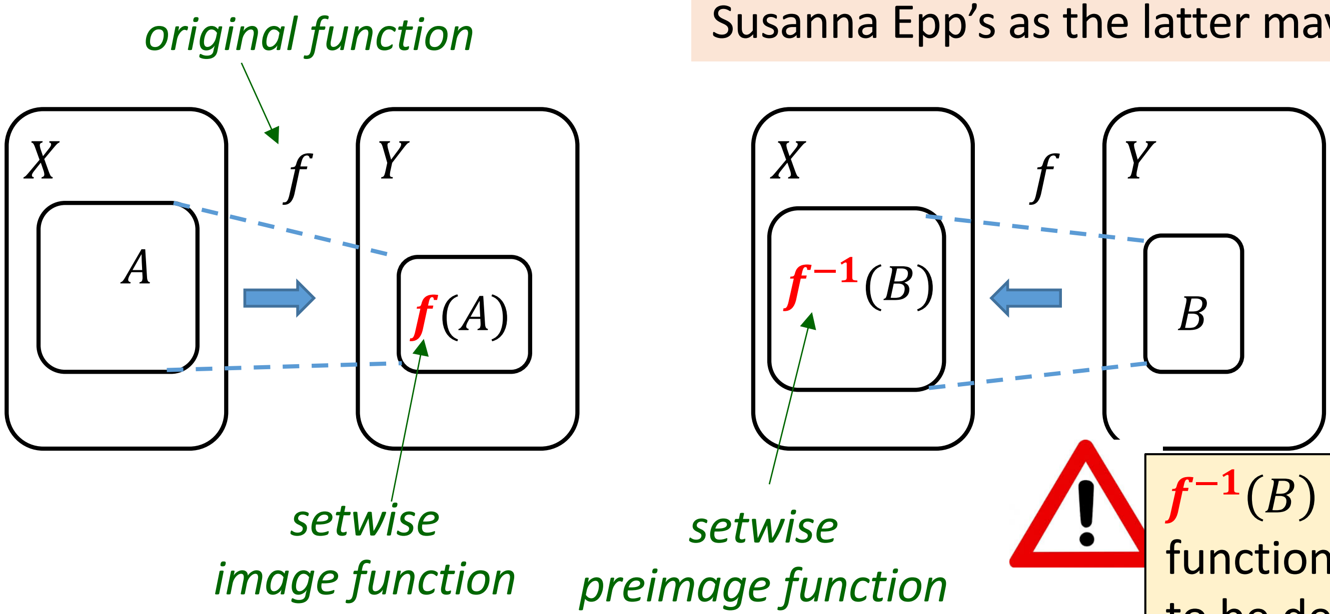
and $\boldsymbol{f}$: $\mathcal{P}(X) \to \mathcal{P}(Y)$ be lifted setwise of f from $\mathcal{P}(X)$ to $\mathcal{P}(Y)$

$\boldsymbol{f}^{-1}$: $\mathcal{P}(Y) \to \mathcal{P}(X)$

- If $A \subseteq X$, then let $\boldsymbol{f}(A) = \{f(x) : x \in A\}$.
- If $B \subseteq Y$, then let $\boldsymbol{f}^{-1}(B) = \{x \in X : f(x) \in B\}$

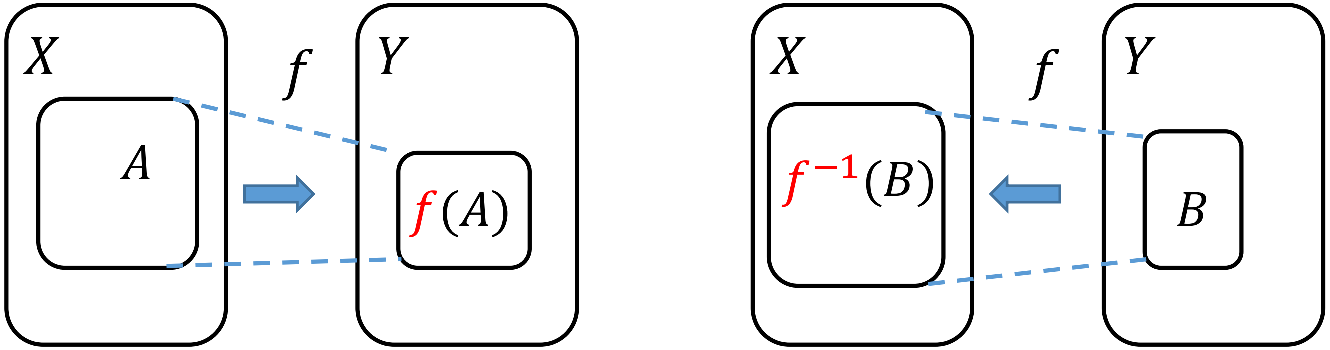
We call $\boldsymbol{f}(A)$ the **(setwise) image** of A, and $\boldsymbol{f}^{-1}(B)$ the **(setwise) preimage** of B under f.

Note: We use different terminologies here from Susanna Epp's as the latter may cause confusion.



$\boldsymbol{f}^{-1}(B)$ is NOT an inverse function! (Inverse function to be defined later.)

Definitions: Setwise image and preimage



Example #4:

A function $g: \mathbb{Z} \to \mathbb{Z}$ is defined by setting $g(x) = x^2 \; \forall x \in \mathbb{Z}$.

What is $g(\{-1,0,1\})$? What is $g^{-1}(\{0,1,2\})$?

$g(\{-1,0,1\}) = \{g(-1), g(0), g(1)\} = \{1,0,1\} = \{0,1\}$.

$g^{-1}(\{0,1,2\}) = \{-1,0,1\}$. (Because $g(0) = 0$; $g(-1) = g(1) = 1$.)

$g^{-1}(\{2\}) = \{\ \}$. (Because $\{x \mid (x,2) \in g\} = \{\}$)

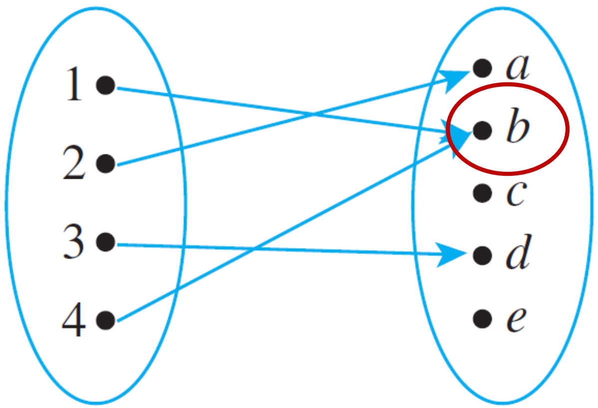
Let $f: X \to Y$ be a function from set X to set Y.

- If $A \subseteq X$, then let $f(A) = \{f(x) : x \in A\}$.
- If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X : f(x) \in B\}$

Definitions: Setwise image and preimage

As the symbol for setwise preimage is $\boldsymbol{f^{-1}}$ is identical to the symbol for inverse function (see section 7.2.4), we use the notation $\boldsymbol{f^{-1}}(\alpha)$ *or* $setwise\_preimage(f)\ (\alpha)$ to denote setwise preimage of a set α (subset of the co-domain), reserving the notation $f^{-1}(x)$ (where x is a member of the co-domain) for the inverse function.

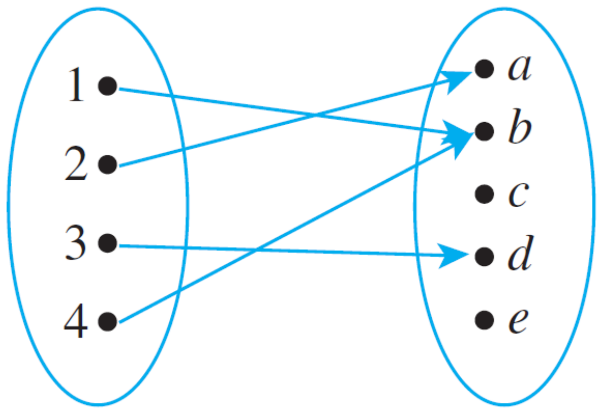
Note that $\boldsymbol{f^{-1}}(\alpha)$ *or* $setwise\_preimage(f)\ (\alpha)$ as a setwise preimage function always exists, whereas inverse function $f^{-1}(x)$ may or may not exists.



Therefore, to denote the setwise preimage of a single element in the co-domain, eg: b, we must write $\boldsymbol{f^{-1}}(\{b\})$ instead of $f^{-1}(b)$. (The latter denotes an inverse function that may not exist.)

$$\boldsymbol{f^{-1}}(\{b\}) = \{1,4\}.$$

Example #5: Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$, and define $f: X \to Y$ by the following arrow diagram:



Let $A = \{1, 4\}$, $B = \{a, b\}$, and $C = \{c, e\}$. Find:

(a) $f(A)$ $\{b\}$

(b) $f(X)$ $\{a, b, d\}$

(c) $f^{-1}(B)$ $\{1,2,4\}$

(d) $f^{-1}(C)$ $\emptyset$

Relation : Domain, Co-domain, Range

Let A and B be sets and R be a relation from A to B.

The **domain** of R, $Dom(R)$, is the set $\{a \in A : aRb \text{ for some } b \in B\}$.

The **co-domain** of R, $coDom(R)$, is the set B.

The **range** of R, $Range(R)$, is the set $\{b \in B: aRb \text{ for some } a \in A\}$.

Domain ⊆ A
Co-domain = B
Range ⊆ Co-domain

Function : Domain, co-domain, range

Let $f: A \to B$ be a function from set A to set B.

- A is the **domain** of f and B the **co-domain** of f.
- The **range** of f is the (setwise) image of A under f:
  $\{b \in B : b = f(a) \text{ for some } a \in A\}$.

Domain = A
Co-domain = B
Range ⊆ Co-domain

Definitions: Domain, co-domain, range

Let $f : A \to B$ be a function from set A to set B.

- A is the **domain** of f and B the **co-domain** of f.
- The **range** of f is the (setwise) image of X under f:
  $\{y \in B : y = f(x)$ for some $x \in A\}$.

Domain = A
Co-domain = B
Range ⊆ Co-domain

Example #6: A function $f : \mathbb{Z} \to \mathbb{Z}$ is defined as:

$$\forall x \in \mathbb{Z}, f(x) = 2x + 1.$$

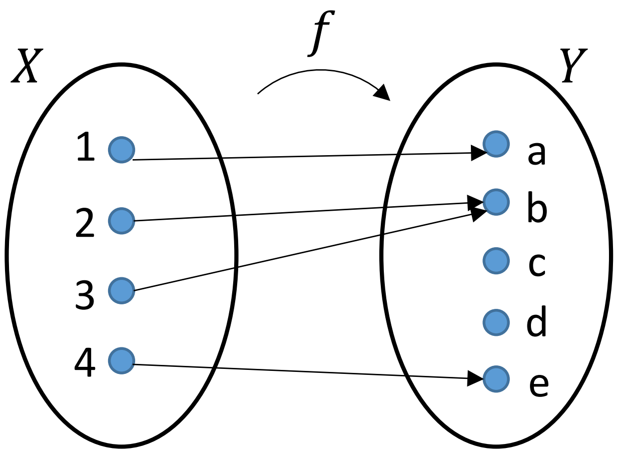
What are the domain, co-domain, and range of f?

Domain: the set of integers, $\mathbb{Z}$.

Co-domain: the set of integers, $\mathbb{Z}$.

Range: the set of odd integers.

Example #7: The function $f: X \to Y$ is shown below.



(a) Represent f as a set of ordered pairs. $\{(1,a),(2,b),(3,b),(4,e)\}$

(b) The domain of f? X or $\{1,2,3,4\}$

(c) The co-domain of f? Y or $\{a,b,c,d,e\}$

(d) The range of f? $\{a,b,e\}$

(e) The image of 4, i.e. $f(4)$? e

(f) The (setwise) image of $\{3,4\}$, i.e. $f(\{3,4\})$? $\{b,e\}$

(g) A pre-image of b? 2 or 3

(h) The (setwise) preimage of $\{b\}$, i.e. $f^{-1}(\{b\})$? $\{2,3\}$

(i) The (setwise) preimage of $\{c,d\}$, i.e. $f^{-1}(\{c,d\})$? $\emptyset$

(j) The (setwise) preimage of $\{a,b,c\}$, i.e. $f^{-1}(\{a,b,c\})$? $\{1,2,3\}$

7.1.2 Sequences and Strings

Definition: Sequence (of infinite length)

A **sequence** $a_0, a_1, a_2, \cdots$ can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$.

In this sense, any function whose domain is $\mathbb{Z}_{\geq m}$ for some $m \in \mathbb{Z}$ represents a sequence.

Example #8: Consider the sequence 2, 3, 5, 9, 17, 33, 65, ... We may represent this sequence by the function $a: \mathbb{Z}_{\geq 0} \to \mathbb{Z}^+$ that satisfies, for each $n \in \mathbb{Z}_{\geq 0}, a(n) = 2^n + 1$.

Definition: Fibonacci Sequence

The **Fibonacci sequence** $F_0, F_1, F_2, \cdots$ is defined by setting, for each $n \in \mathbb{Z}_{\geq 0}$, $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

Fibonacci sequence: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, …

Example #9: We may represent the Fibonacci sequence $F_0, F_1, F_2, \cdots$ by the function $F: \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ that satisfies, for each $n \in \mathbb{Z}_{\geq 0}$,

$$F(0) = 0 \text{ and } F(1) = 1 \text{ and } F(n+2) = F(n+1) + F(n).$$

base defns

inductive defn

$$F(n) = y \;\; \boldsymbol{st} \; F(0) = 0 \wedge F(1) = 1 \wedge \forall n \in \mathbb{Z}_{\geq 0} \; F(n+2) = F(n+1) + F(n).$$

Definition: String (of finite length)

Let A be a set. A **string** or a word over A is an expression of the form $a_0a_1a_2\cdots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, a_2, \cdots, a_{l-1} \in A$.

Here l is called the **length** of the string. The **empty string** ε is the string of length 0.

Example #10: Let $A = \{s, u\}$. Some strings over A are $s, ssuu$, $susuussu$ and $uuuuuuu$ with lengths 1, 4, 8 and 7 respectively.

One can represent a string $a_0a_1a_2\cdots a_{l-1}$ over A by the function $a: \{0,1,\dots,l-1\} \to A$ satisfying $a(n) = a_n$ for all $n \in \{0,1,\dots,l-1\}$.

Every function $a: \{m, m+1, \dots, m+l-1\} \to A$ where $m \in \mathbb{Z}$ and $l \in \mathbb{Z}_{\geq 0}$ represents a string of length l over A, namely, $a(m)\, a(m+1) \dots a(m+l-1)$.

Equality of Sequences

Given two sequences $a_0, a_1, a_2, \cdots$ and $b_0, b_1, b_2, \cdots$ defined by the functions $a(n) = a_n$ and $b(n) = b_n$ respectively for every $n \in \mathbb{Z}_{\geq 0}$, we say that the two sequences are equal if and only if $a(n) = b(n)$ for every $n \in \mathbb{Z}_{\geq 0}$.

A^∞ **or Seq(A)** denote the set of all (infinite) sequences over A
= is a relation with type A^∞ x A^∞

Equality of Strings

Given two strings $s_1 = a_0 a_1 a_2 \cdots a_{l-1}$ and $s_2 = b_0 b_1 b_2 \cdots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that

$s_1 = s_2$ if and only if $a_i = b_i$ for all $i \in \{0,1,2, \dots, l-1\}$.

A^* **or Str(A)** denote the set of all (finite) strings over A
= is a relation with type A^* x A^*

7.1.3 Function Equality

Theorem 7.1.1 Function Equality

Two functions $f: A \to B$ and $g: C \to D$ are equal, i.e. $f = g$, iff (i) $A = C$ and $B = D$, and (ii) $f(x) = g(x)\ \forall x \in A$.

Example #11: Let $X = \{0,1,2\}$ and define functions f and g on X as follows: $\forall x \in X$,

$$f(x) = (x^2 + x + 1)\ mod\ 3 \quad \text{and} \quad g(x) = (x+2)^2\ mod\ 3$$

Is $f = g$?

Note: $a\ mod\ b$ computes the remainder of $a \div b$.

Yes.

x	x^2+x+1	$f(x) = (x^2+x+1)\ mod\ 3$	$(x+2)^2$	$g(x) = (x+2)^2\ mod\ 3$
0	1	$1\ mod\ 3 = 1$	4	$4\ mod\ 3 = 1$
1	3	$3\ mod\ 3 = 0$	9	$9\ mod\ 3 = 0$
2	7	$7\ mod\ 3 = 1$	16	$16\ mod\ 3 = 1$

Theorem 7.1.1 Function Equality

Two functions $f: A \to B$ and $g: C \to D$ are equal, i.e. $f = g$, iff (i) $A = C$ and $B = D$, and (ii) $f(x) = g(x)\ \forall x \in A$.

Example #12: Let $f: \{0,2\} \to \mathbb{Z}$ and $g: \{0,2\} \to \mathbb{Z}$ defined by setting, for all $x \in \{0,2\}$, $f(x) = 2x$ and $g(x) = x^2$.

Is $f = g$?

Yes. Their domains are the same, their co-domains are the same, and $f(x) = g(x)$ for every $x \in \{0,2\}$.

Example #13: Let $f: \mathbb{Z} \to \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{Q}$ defined by setting, for all $x \in \mathbb{Z}$, $f(x) = x^3 = g(x)$. Is $f = g$?

No, because their co-domains are different.

7.2 Injections, Surjections, Bijections and Inverse Functions

7.2.1 Injections (One-to-One Functions)

Definition: Injection (one-to-one function)

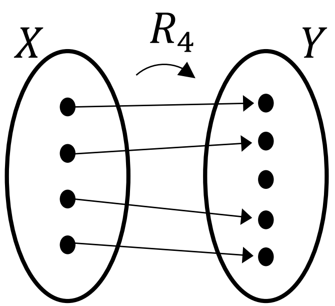
A function $f: X \to Y$ is **injective** (or **one-to-one**) iff

$$\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

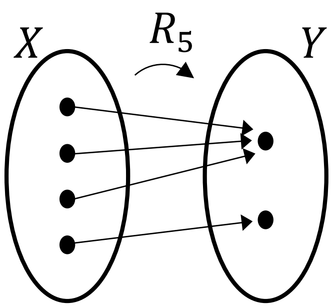
or, equivalently (contrapositive), $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.
An injective function is called an **injection**.

Property of functions $\forall f,\quad x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$

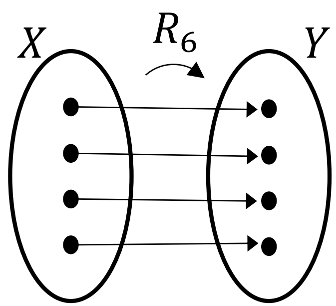
Which of the following is/are injections?



Injection



Not injection



Injection

A function $f: X \to Y$ is **injective** iff
$\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

A function $f: X \to Y$ is **not injective** iff
$\exists x_1, x_2 \in X\ (f(x_1) = f(x_2) \wedge x_1 \neq x_2)$.

Example #14: Define a function $f: \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Is f injective?

Yes. Proof:

1. Let $x_1, x_2 \in \mathbb{Q}$ such that $f(x_1) = f(x_2)$.
2. Then $3x_1 + 1 = 3x_2 + 1$.
3. So $x_1 = x_2$.

Example #15: Define $g: \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Is g injective?

No. $g(1) = 1^2 = 1 = (-1)^2 = g(-1)$, but $1 \neq -1$.

7.2.2 Surjections (Onto Functions)

Definition: Surjection (onto function)

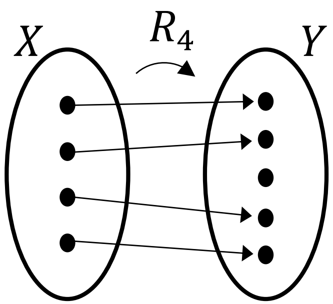
A function $f: X \to Y$ is **surjective** (or **onto**) iff

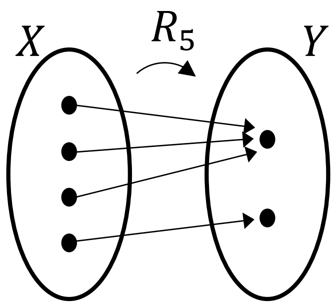
$$\forall y \in Y\ \exists x \in X\ \big(y = f(x)\big).$$

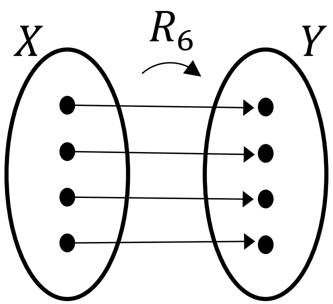
Every element in the co-domain has at least one preimage. So, range = co-domain.

A surjective function is called a **surjection**.

Which of the following is/are surjections?







Not surjection

Surjection

Surjection

Surjections (Onto Functions)

A function $f: X \to Y$ is **surjective** iff $\forall y \in Y\ \exists x \in X\ \big(y = f(x)\big)$.

A function $f: X \to Y$ is **not surjective** iff $\exists y\ \in Y\ \forall x \in X\ \big(y \neq f(x)\big)$.

Example #16: Define a function $f: \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Is f surjective?

Yes. Proof:

1. Take any $y \in \mathbb{Q}$.
2. Let $x = (y - 1)/3$.
3. Then $x \in \mathbb{Q}$ and $f(x) = 3x + 1 = 3\left(\frac{y-1}{3}\right) + 1 = y$.

Example #17: Define $g: \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Is g surjective?

No.
$g(x) = x^2 \geq 0 > -1$ for all $x \in \mathbb{Z}$.
So $g(x) \neq -1$ for all $x \in \mathbb{Z}$, although $-1 \in \mathbb{Z}$.

7.2.3 Bijections (One-to-One Correspondences)

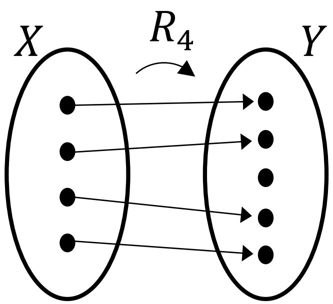
Definition: Bijection (one-to-one correspondence)

A function $f: X \to Y$ is **bijective** iff f is injective and surjective, i.e.

$$\forall y \in Y \; \exists! \, x \in X \; \big(y = f(x)\big).$$

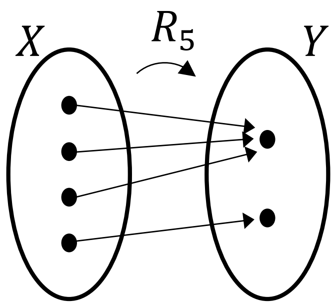
A bijective function is called a **bijection** or **one-to-one correspondence**.

Which of the following is/are bijections?



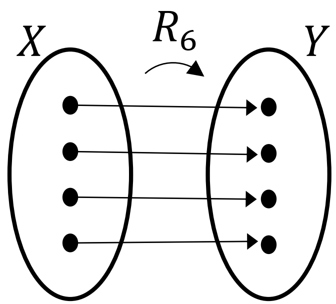
Injection

Not surjection



Not injection

Surjection



Injection

Surjection

Bijection

Bijections (One-to-One Correspondences)

A function $f: X \to Y$ is:

- injective iff $\forall x_1, x_2 \in X \; (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$;
- surjective iff $\forall y \in Y \; \exists x \in X \; \big(y = f(x)\big)$;
- bijective iff $\forall y \in Y \; \exists!\, x \in X \; \big(y = f(x)\big)$.

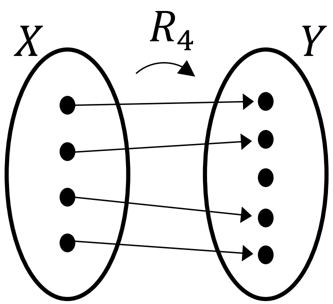
(Injective) Informally, every element in the codomain must have **at most one arrow** going into it.

$\wedge$

(Surjective) Informally, every element in the codomain must have **at least one arrow** going into it.

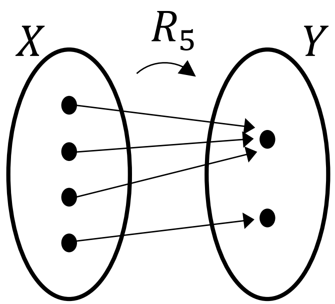
$\equiv$

(Bijective) Informally, every element in the codomain must have **exactly one arrow** going into it.



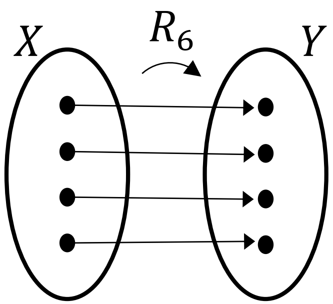
Injection

Not surjection



Not injection

Surjection



Injection

Surjection

Bijection

7.2.4 Inverse Functions

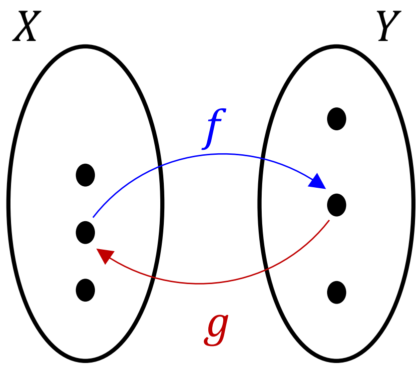
If f is a bijection from X to Y, then there is a function from Y to X that "undoes" the action of f; that is, it sends each element of Y back to the element of X that it came from. This function is called the *inverse function* for f, denoted as f^{-1}.

Definition: Inverse function

Let $f: X \to Y$. Then $g: Y \to X$ is an **inverse** of f iff

$$\forall x \in X\ \forall y \in Y\ \big(y = f(x) \Leftrightarrow x = g(y)\big).$$

We denote the inverse of f as f^{-1}.



Definition: Inverse function

Let $f: X \to Y$. Then $g: Y \to X$ is an **inverse** of f iff

$$\forall x \in X\ \forall y \in y\ \big(y = f(x) \Leftrightarrow x = g(y)\big).$$

We denote the inverse of f as f^{-1}.

Example #18: Define $f: \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Note that for all $x, y \in \mathbb{Q}$, $y = 3x + 1 \Leftrightarrow x = (y - 1)/3$.

Let $g: \mathbb{Q} \to \mathbb{Q}$ such that $g(y) = (y - 1)/3$ for all $y \in \mathbb{Q}$. Then the above tells us $\forall x, y \in \mathbb{Q}\ \big(y = f(x) \Leftrightarrow x = g(y)\big)$.

Therefore, g is the inverse of f.

Proposition: Uniqueness of inverses

If g_1 and g_2 are inverses of $f: X \to Y$, then $g_1 = g_2$.

Proof:

1. Note that $g_1, g_2: Y \to X$.
2. Since g_1 and g_2 are inverses of f, for all $x \in X$ and $y \in Y$, $x = g_1(y) \Leftrightarrow y = f(x) \Leftrightarrow x = g_2(y)$.
3. Therefore $g_1 = g_2$.

7.2.5 Bijectivity and Invertibility

Theorem 7.2.3

If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection.
In other words, $f: X \to Y$ is bijective iff f has an inverse.

Proof: ($f: X \to Y$ is bijective iff f has an inverse)

1. ("if") Suppose f has an inverse, say $g: Y \to X$.
   - 1.1. We show injectivity of f.
     injective(f) iff $\forall x_1, x_2 \in X\, (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$
     - 1.1.1. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.
     - 1.1.2. Define $y = f(x_1) = f(x_2)$.
     - 1.1.3. Then $x_1 = g(y)$ and $x_2 = g(y)$ as g is an inverse of f.
     - 1.1.4. Hence $x_1 = x_2$.
   - 1.2. We show surjectivity of f.
     surjective (f) iff $\forall y \in Y\, \exists x \in X\, (y = f(x))$
     - 1.2.1. Let $y \in Y$.
     - 1.2.2. Define $x = g(y)$.
     - 1.2.3. Then $y = f(x)$ as g is an inverse of f.
   - 1.3. Therefore f is bijective.

Theorem 7.2.3

If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection.
In other words, $f: X \to Y$ is bijective iff f has an inverse.

Proof: ($f: X \to Y$ is bijective iff f has an inverse)

1. (“if”) Suppose f has an inverse, say $g: Y \to X$.
2. (“only if”) Suppose f is bijective.
   2.1. Then $\forall y \in Y\ \exists!\, x \in X\ \big(y = f(x)\big)$ by the definition of bijection.
   2.2. Define the function $g: Y \to X$ by setting $g(y)$ to be the unique $x \in X$ such that $y = f(x)$ for all $y \in Y$.
   2.3. This g is well defined and is an inverse of f by the definition of inverse functions.
3. Therefore $f: X \to Y$ is bijective iff f has an inverse.

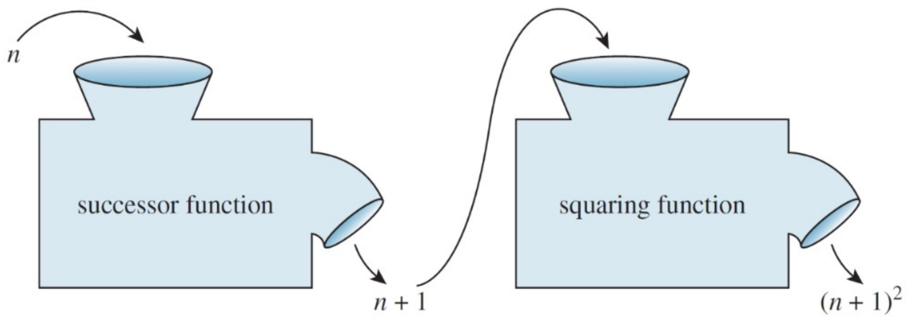
7.3 Composition of Functions

7.3.1 Composition of Functions

Consider two functions, the successor function and the squaring function, defined from $\mathbb{Z}$ to $\mathbb{Z}$, and imagine that each is represented by a machine.

If the two machines are hooked up so that the output from the successor function is used as input to the squaring function, then they work together to operate as one larger machine.

In this larger machine, an integer n is first increased by 1 to obtain $n + 1$; then the quantity $n + 1$ is squared to obtain $(n + 1)^2$.



Combining functions in this way is called *composing* them; the resulting function is called the *composition* of the two functions.

Definition: Composition of Functions

Let $f: X \to Y$ and $g: Y \to Z$ be functions.

Define a new function $g \circ f: X \to Z$ as follows:

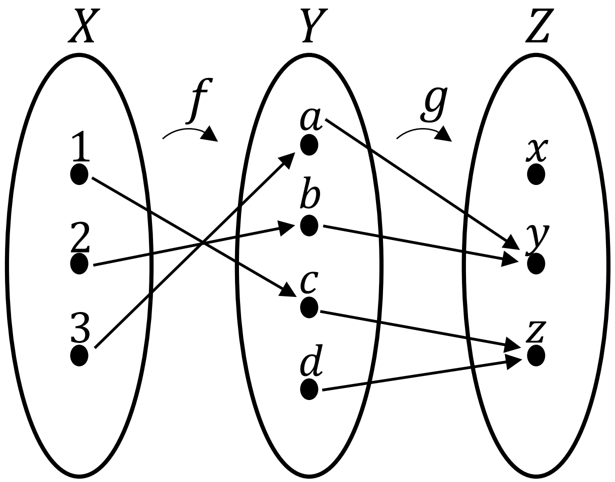
$$(g \circ f)(x) = g\big(f(x)\big)\ \forall x \in X.$$

where $g \circ f$ is read "g circle f" and $g\big(f(x)\big)$ is read "g of f of x".

The function $g \circ f$ is called the **composition** of f and g.

Composition of Functions

Example #19: Let $X = \{1, 2, 3\}, Y = \{a, b, c, d\}$ and $Z = \{x, y, z\}$.
Define functions $f: X \to Y$ and $g: Y \to Z$ by the arrow diagrams below.

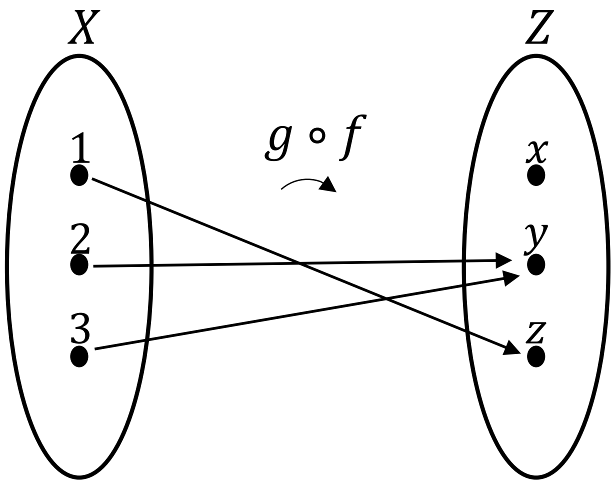


Draw the arrow diagram for $g \circ f$.

What is the type of $g \circ f$?

$g \circ f : X \to Z$

What is the range of $g \circ f$?



$$(g \circ f)(1) = g(f(1)) = g(c) = z$$
$$(g \circ f)(2) = g(f(2)) = g(b) = y$$
$$(g \circ f)(3) = g(f(3)) = g(a) = y$$

Therefore the range of $g \circ f$ is $\{y, z\}$.

7.3.2 Composition with the Identity Function

The identity function on a set X, id_X, is the function from X to X defined by $id_X(x) = x$ for all $x \in X$.

Let $f: X \to Y$.

(1) $f \circ id_X = f$ because

- Domains of $f \circ id_X$ and f are both X;
- Co-domains of $f \circ id_X$ and f are both Y;
- $(f \circ id_X)(x) = f\big(id_X(x)\big) = f(x)$ for all $x \in X$.

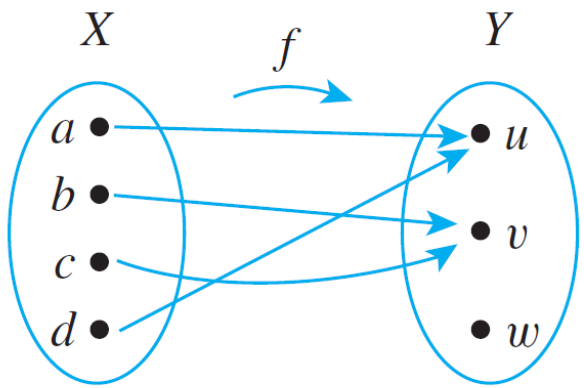
(2) $id_Y \circ f = f$ because

- Domains of $id_Y \circ f$ and f are both X;
- Co-domains of $id_Y \circ f$ and f are both Y;
- $(id_Y \circ f)(x) = id_Y\big(f(x)\big) = f(x)$ for all $x \in X$.

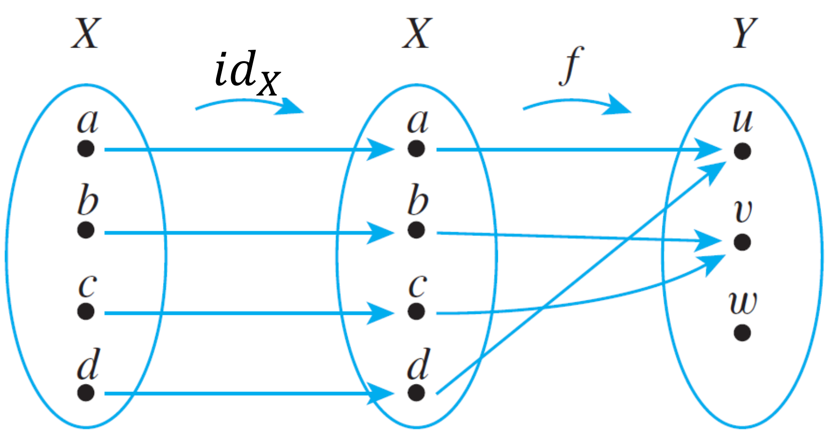
$$
\begin{tikzcd}
X \arrow[r, "id_X"] \arrow[dr, "f"'] & X \arrow[d, "f"'] \arrow[dr, "f"] & \\
 & Y \arrow[r, "id_Y"'] & Y
\end{tikzcd}
$$

Example #20: Let $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$, and suppose $f: X \to Y$ is given by the arrow diagram:

$$f \circ id_X = f$$



Find $f \circ id_X$

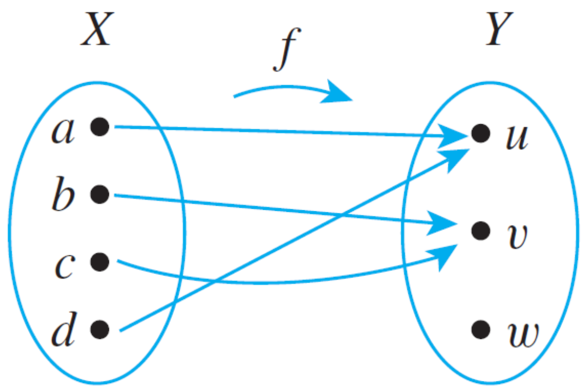


$(f \circ id_X)(a) = f\big(id_X(a)\big) = f(a) = u$
$(f \circ id_X)(b) = f\big(id_X(b)\big) = f(b) = v$
$(f \circ id_X)(c) = f\big(id_X(c)\big) = f(c) = v$
$(f \circ id_X)(d) = f\big(id_X(d)\big) = f(d) = u$

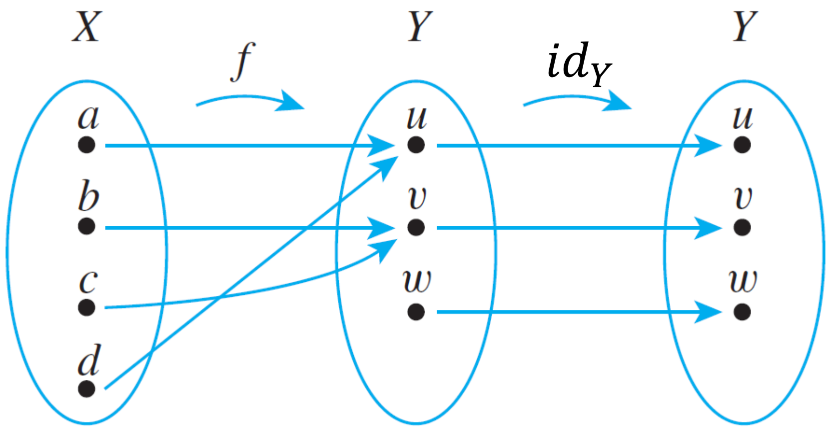
$$(f \circ id_X)(x) = f(x).$$

Example #21: Let $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$, and suppose $f: X \to Y$ is given by the arrow diagram:

$$id_Y \circ f = f$$



Find $id_Y \circ f$



$$(id_Y \circ f)(a) = id_Y(f(a)) = f(a) = u$$
$$(id_Y \circ f)(b) = id_Y(f(b)) = f(b) = v$$
$$(id_Y \circ f)(c) = id_Y(f(c)) = f(c) = v$$
$$(id_Y \circ f)(d) = id_Y(f(d)) = f(d) = u$$

$$(id_Y \circ f)(x) = f(x).$$

Theorem 7.3.1 Composition with an Identity Function

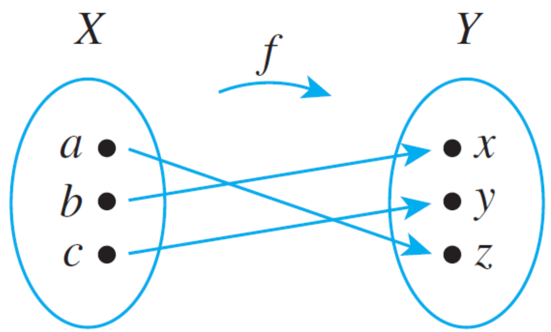
If f is a function from a set X to a set Y, and id_X is the identity function on X, and id_Y is the identity function on Y, then

$$f \circ id_X = f \text{ and}$$

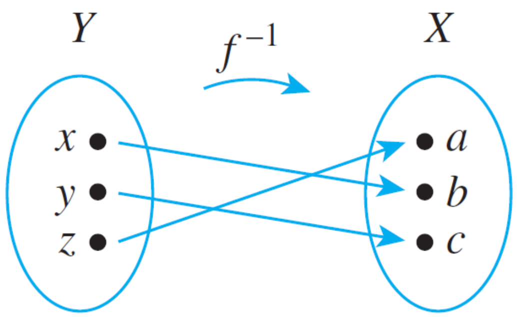
$$id_Y \circ f = f$$

7.3.3 Composing a Function with Its Inverse

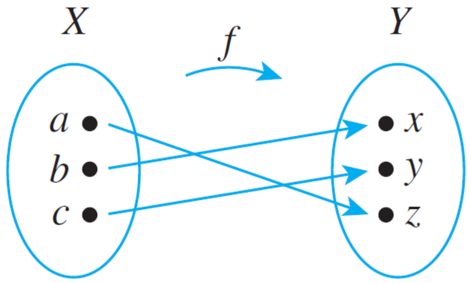
Example #22: Let $X = \{a, b, c\}$ and $Y = \{x, y, z\}$. Define $f: X \to Y$ by the following arrow diagram.

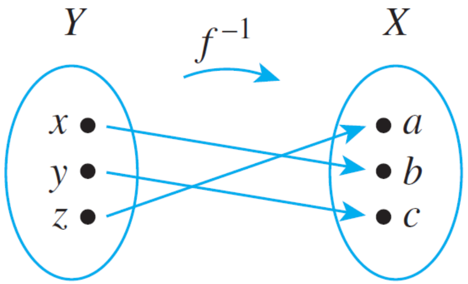


Then f is a bijection. Thus f^{-1} exists and is found by tracing the arrows backwards, as shown below.



Now $f^{-1} \circ f$ is found by following the arrows from X to Y by f and back to X by f^{-1}.





$$(f^{-1} \circ f)(a) = f^{-1}\big(f(a)\big) = f^{-1}(z) = a$$
$$(f^{-1} \circ f)(b) = f^{-1}\big(f(b)\big) = f^{-1}(x) = b$$
$$(f^{-1} \circ f)(c) = f^{-1}\big(f(c)\big) = f^{-1}(y) = c$$

Therefore, $f^{-1} \circ f = id_X$.

Similarly, $f \circ f^{-1} = id_Y$.

Theorem 7.3.2 Composition of a Function with Its Inverse

If $f: X \to Y$ is a bijection with inverse function $f^{-1}: Y \to X$, then
$f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$

7.3.4 Associativity of Function Composition

Function composition. Let $f: X \to Y$ and $g: Y \to Z$.
Then $g \circ f: X \to Z$ such that for every $x \in X$, $(g \circ f)(x) = g\big(f(x)\big)$.

Theorem: Associativity of Function Composition

Let $f: A \to B$, $g: B \to C$ and $h: C \to D$. Then

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Function composition is associative.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "g \circ f"'] & B \arrow[d, "g"] \arrow[dr, "h \circ g"] & \\
& C \arrow[r, "h"'] & D
\end{tikzcd}$$

Proof:

1. The domains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both A.
2. The codomains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both D.
3. For every $x \in A$,

$$\boxed{\text{Defn}: (g \circ f)(x) = g\big(f(x)\big)\ \forall x \in X}$$

$$\big((h \circ g) \circ f\big)(x) = (h \circ g)\big(f(x)\big) = h\Big(g\big(f(x)\big)\Big) = h\big((g \circ f)(x)\big) = \big(h \circ (g \circ f)\big)(x).$$

7.3.5 Noncommutativity of Function Composition

Function composition. Let $f: X \to Y$ and $g: Y \to Z$.
Then $g \circ f: X \to Z$ such that for every $x \in X$, $(g \circ f)(x) = g(f(x))$.

Example #23: Let $f, g: \mathbb{Z} \to \mathbb{Z}$ such that for every $x \in \mathbb{Z}$,

$$f(x) = 3x \text{ and } g(x) = x + 1.$$

Then for every $x \in \mathbb{Z}$,

$$(g \circ f)(x) = g(f(x)) = g(3x) = 3x + 1$$

and

$$(f \circ g)(x) = f(g(x)) = f(x + 1) = 3(x + 1).$$

Note that $(g \circ f)(0) = 1 \neq 3 = (f \circ g)(0)$.

7.3.6 Composition of Injections

Example #24:

Let $X = \{a, b, c\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3, 4, 5\}$, and define injections $f: X \to Y$ and $g: Y \to Z$ as shown in the arrow diagrams of Figure 7.3.1.

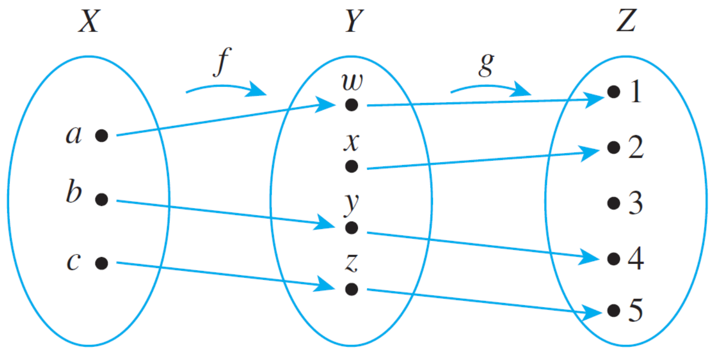


Figure 7.3.1

Then $g \circ f$ is the function with the arrow diagram shown in Figure 7.3.2.

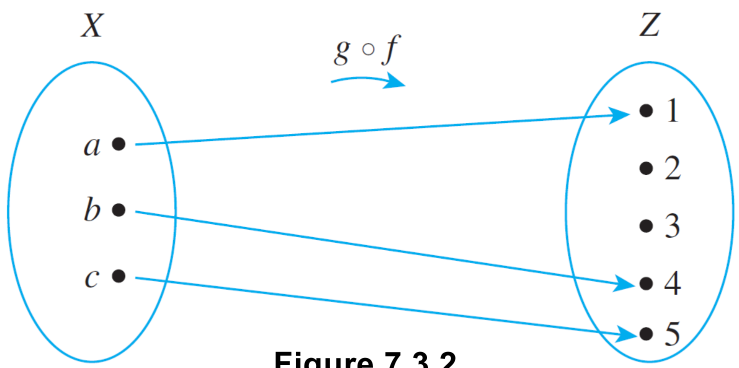


Figure 7.3.2

Is $g \circ f$ injective? Yes.

Theorem 7.3.3

If $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective.

injective(*g*) iff $\forall y_1, y_2 \in Y\ (g(y_1) = g(y_2) \Rightarrow y_1 = y_2)$.

injective(*f*) iff $\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

Proof:

1. Suppose $f: X \to Y$ and $g: Y \to Z$ are injections and let $x_1, x_2 \in X$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$.
2. Then $(g(f(x_1)) = g(f(x_2))$ by the definition of function composition.
3. Since g is injective, so $f(x_1) = f(x_2)$ by the definition of injection.
4. Since f is injective, so $x_1 = x_2$ by the definition of injection.
5. Therefore $g \circ f$ is injective.

Function -> Every input has a unique output

Injection -> Output has a unique input (if there exists one)

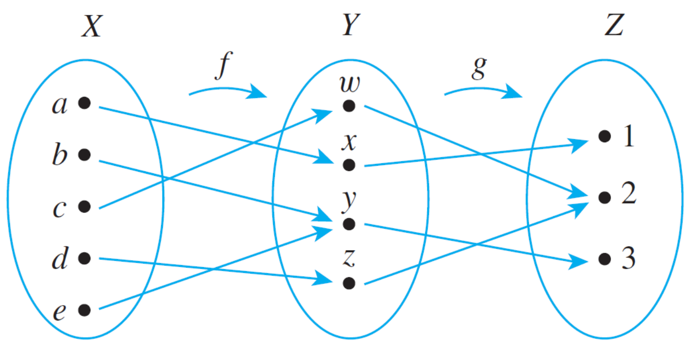
Surjection -> Every output has an input

Bijection -> Every output has a unique input

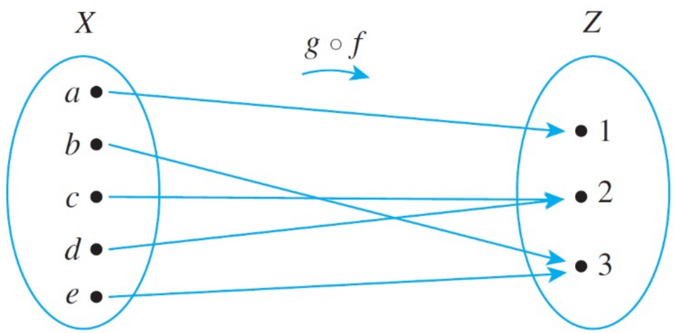
7.3.7 Composition of Surjections

Example #25:

Let $X = \{a, b, c, d, e\}$, $Y = \{w, x, y, z\}$, and $Z = \{1, 2, 3\}$, and define surjections $f: X \to Y$ and $g: Y \to Z$ as shown in the arrow diagrams on the right.



Then $g \circ f$ is the function with the arrow diagram on the right.



Is $g \circ f$ surjective? Yes.

Theorem 7.3.4

If $f: X \to Y$ and $g: Y \to Z$ are both surjective, then $g \circ f$ is surjective.

surjective(g) iff $\forall z \in Z\ \exists y \in Y\ \big(z = g(y)\big)$.

surjective(f) iff $\forall y \in Y\ \exists x \in X\ \big(y = f(x)\big)$.

Proof:

1. Suppose $f: X \to Y$ and $g: Y \to Z$ are surjections and let $z \in Z$.
2. Since g is surjective, so there is an element $y \in Y$ such that $g(y) = z$ by the definition of surjection.
3. Since f is surjective, so there is an element $x \in X$ such that $f(x) = y$ by the definition of surjection.
4. Hence there exists an element $x \in X$ such that $(g \circ f)(x) = g\big(f(x)\big) = g(y) = z$.
5. Therefore $g \circ f$ is surjective.

7.4 Addition and Multiplication Functions on $\mathbb{Z}_n$

7.4.1 Definitions (from Lecture #6)

Definition: Congruence

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$. In other words, $n \mid (a - b)$.

In this case, we write $a \equiv b \pmod{n}$.

Proposition

Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$.

Definition: Equivalence Class

Suppose A is a set and $\sim$ is an equivalence relation on A. The **equivalence class** of $a \in A$, is

$$[a]_\sim = \{x \in A : a \sim x\}.$$

Definition: Set of equivalence classes

Let A be a set and $\sim$ be an equivalence relation on A. Denote by $A/\sim$ the set of all equivalence classes with respect to $\sim$, i.e.,

$$A/\sim\ = \{[x]_\sim : x \in A\}.$$

We may read $A/\sim$ as "the quotient of A by $\sim$".

Now, we introduce a notation $\mathbb{Z}_n$:

The quotient $\mathbb{Z}/\sim_n$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$.

Definition: $\mathbb{Z}_n$

The quotient $\mathbb{Z}/{\sim_n}$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$.

From Lecture #6:

Congruence modulo 2

$\mathbb{Z}$

:	:
-4	-3
-2	-1
0	1
2	3
4	5
:	:

Partition of $\mathbb{Z}$:
$\left\{\begin{matrix} \{2k : k \in \mathbb{Z}\}, \\ \{2k+1 : k \in \mathbb{Z}\} \end{matrix}\right\}$

Congruence modulo 3

$\mathbb{Z}$

:	:	:
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
:	:	:

Partition of $\mathbb{Z}$:
$\left\{\begin{matrix} \{3k : k \in \mathbb{Z}\}, \\ \{3k+1 : k \in \mathbb{Z}\}, \\ \{3k+2 : k \in \mathbb{Z}\} \end{matrix}\right\}$

Congruence modulo 4

$\mathbb{Z}$

:	:	:	:
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
:	:	:	:

Partition of $\mathbb{Z}$:
$\left\{\begin{matrix} \{4k : k \in \mathbb{Z}\}, \\ \{4k+1 : k \in \mathbb{Z}\}, \\ \{4k+2 : k \in \mathbb{Z}\}, \\ \{4k+3 : k \in \mathbb{Z}\} \end{matrix}\right\}$

$$\mathbb{Z}_2 = \{\{2k : k \in \mathbb{Z}\}, \{2k+1 :\ k \in \mathbb{Z}\}\}$$

$$\mathbb{Z}_3 = \{\{3k : k \in \mathbb{Z}\}, \{3k+1 :\ k \in \mathbb{Z}\}, \{3k+2 :\ k \in \mathbb{Z}\}\}$$

$$\mathbb{Z}_4 = \{\{4k : k \in \mathbb{Z}\}, \{4k+1 :\ k \in \mathbb{Z}\}, \{4k+2 :\ k \in \mathbb{Z}\}, \{4k+3 :\ k \in \mathbb{Z}\}\}$$

7.4.2 Addition and Multiplication on $\mathbb{Z}_n$

Definition: Addition and Multiplication on $\mathbb{Z}_n$

Define addition $+$ and multiplication $\cdot$ on $\mathbb{Z}_n$ as follows:

whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y]$$

Example #26:

Take $[0], [1] \in \mathbb{Z}_3$,

Then $[0] + [1] = [0 + 1] = [1]$ (which is $\{\dots, -5, -2, 1, 4, 7, \dots\}$)

and $[0] \cdot [1] = [0 \cdot 1] = [0]$ (which is $\{\dots, -6, -3, 0, 3, 6, \dots\}$).

base functions on $\mathbb{Z}$	$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$	$\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$
derived functions on $\mathbb{Z}_n$	$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$	$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

Addition and Multiplication on $\mathbb{Z}_n$

Proposition: Addition on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$([x_1], [y_1]) = ([x_2], [y_2]) \Rightarrow [x_1] + [y_1] = [x_2] + [y_2].$$

General Well-Defined Function Property

$$\forall\, x_1, x_2 \in X, \forall\, f : X \to Y,\ x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$$

Well-Defined Property wrt Equiv Relation ~

$$\forall\, x_1, x_2 \in X, \forall\, f : X \to Y,\ x_1 \sim x_2 \Rightarrow f(x_1) \sim f(x_2)$$

Lemma Rel.1 Equivalence Classes

Let $\sim$ be an equivalence relation on a set X. The following are equivalent for all $x, y \in X$. (i) $x \sim y$; (ii) $[x] = [y]$; (iii) $[x] \cap [y] \neq \emptyset$.

Well-Defined Property wrt Equiv Class [x]

$$\forall\, x_1, x_2 \in X, \forall\, f : X \to Y,\ [x_1] = [x_2] \Rightarrow [f(x_1)] = [f(x_2)]$$

Proposition: Addition on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2].$$

Defn $\sim n$ $[x_1]{\sim}n = [x_2]{\sim}n$ iff $\exists k\ x_1 - x_2 = nk$

Defn $\sim n$ $[y_1]{\sim}n = [y_2]{\sim}n$ iff $\exists l\ y_1 - y_2 = nl$

Proof:

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence.
3. Use the definition of congruence to find $k, l \in \mathbb{Z}$ such that

   $$x_1 - x_2 = nk \text{ and } y_1 - y_2 = nl.$$
4. Note that $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = nk + nl = n(k + l)$.

   Defn $\sim n$ $[x_1 + y_1]{\sim}n = [x_2 + y_2]{\sim}n$ iff $\exists m\ (x_1 + y_1) - (x_2 + y_2) = nm$
5. So $[x_1 + y_1] = [x_2 + y_2]$ by the definition of congruence mod n.

   Defn $+$ $[x_1], [y_1] \in \mathbb{Z}_n$ => $[x_1] + [y_1] = [x_1 + y_1]$

   Defn $+$ $[x_2], [y_2] \in \mathbb{Z}_n$ => $[x_2] + [y_2] = [x_2 + y_2]$
6. From Defn of $+$, $([x_1] + [y_1] = [x_1 + y_1]) \wedge ([x_2 + y_2] = [x_2] + [y_2])$
7. From (5) and (6), therefore $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$.

Proposition: Multiplication on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \Rightarrow [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

Proof:

Defn $\sim n$ $[x_1]\sim n = [x_2]\sim n$ iff $\exists k\ x_1 - x_2 = nk$

Defn $\sim n$ $[y_1]\sim n = [y_2]\sim n$ iff $\exists l\ y_1 - y_2 = nl$

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence.
3. Use the definition of congruence to find $k, l \in \mathbb{Z}$ such that

   $$x_1 - x_2 = nk \text{ and } y_1 - y_2 = nl.$$

4. Note that $(x_1 \cdot y_1) - (x_2 \cdot y_2) = (nk + x_2) \cdot (nl + y_2) - (x_2 \cdot y_2)$

   $= n(nkl + ky_2 + lx_2)$, where $(nkl + ky_2 + lx_2) \in \mathbb{Z}$ (by closure of integer addition)

   Defn $\sim n$ $[x_1 \cdot y_1]\sim n = [x_2 \cdot y_2]\sim n$ iff $\exists m\ (x_1 \cdot y_1) - (x_2 \cdot y_2) = nm$

5. So $[\,x_1 \cdot y_1] = [x_2 \cdot y_2]$ by the definition of congruence mod n.

   Defn $\cdot$ $[x_1], [y_1] \in \mathbb{Z}_n$ => $[x_1] \cdot [y_1] = [x_1 \cdot y_1]$

   Defn $\cdot$ $[x_2], [y_2] \in \mathbb{Z}_n$ => $[x_2] \cdot [y_2] = [x_2 \cdot y_2]$

6. By Defn of $\cdot$, we have $([x_1] \cdot [y_1] = [x_1 \cdot y_1]) \wedge ([x_2 \cdot y_2] = [x_2] \cdot [y_2])$
7. Therefore, $[x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$ from (5) and (6) .

Definition: Function

A function f from a set X to a set Y, denoted $f: X \to Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X\ \exists y \in Y\ (x, y) \in f$.

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y \Big(\big((x, y_1) \in f \wedge (x, y_2) \in f\big) \to y_1 = y_2\Big)$.

(That is, the y in (F1) is unique.)

Definition: Function

A function f from a set X to a set Y, denoted $f: X \to Y$, is *well-defined*, if it has the following deterministic property:

(F3) $\forall x_1, x_2 \in X\ (x_1 = x_2 \to f(x_1) = f(x_2))$.

Exercise : F1 $\wedge$ F2 $\Leftrightarrow$ F3

Which of the following statements are true about non-empty partial order relations?

(i) It is not possible to have an element that is both smallest and largest.

(ii) It is possible to have an element that is both maximal and minimal but neither largest nor smallest.

(iii) Different maximal elements are comparable to each other.

(iv) It is possible to not have any maximal or minimal elements.

A. Only (ii).

B. Only (i) and (ii).

C. Only (ii) and (iv).

D. Only (ii), (iii) and (iv).

E. None of the options (A), (B), (C), (D) is correct.

Consider the following statements about relations on any <u>non-empty set</u>:

(i) Every asymmetric relation is antisymmetric.
(ii) If a relation is not reflexive then it is not asymmetric.
(iii) If a relation is not reflexive then it is asymmetric.
(iv) There are no relations that are both an equivalence relation and a partial order.

Which of the above statements are true?

Note: Asymmetry is defined in Tutorial 5 as follows:

A binary relation R on a set A is asymmetric iff $\forall x, y \in A\ (xRy \Rightarrow y \not R x)$.

A. Only (i).
B. Only (ii).
C. Only (i) and (iv).
D. Only (ii) and (iii).
E. None of the options (A), (B), (C), (D) is correct.