1) Sets and Functions

1.1 Sets

Defn: A set is a "collection" of "objects," called <u>elements</u>, <u>members</u> or <u>points</u>.

Examples: $\mathbb{N}$ (natural numbers), $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational) and $\mathbb{R}$ (real numbers) are <u>all sets</u>.

Notation: Sets denoted by curly brackets "{" and "}", particularly at point of first definition. Afterwards, sets are usually reffered by a capital letter $A, B, C, \ldots$

Special sets get special symbols like $\mathbb{R}$.

Examples: $\{a, b, c\}$ or $\{1, 2, 3, 4\}$ or $\{x, a, y, 3\}$ etc.

Notation Members of a set are sometimes presented as a (finite or infinite) list

$\{a, b, c\}$ (finite)

$\{a, b, c, \ldots\}$ (infinite)

Sets can also be defined by some property $P(x)$:

$$\{x \mid P(x)\}$$

also written with a colon:

$$\{x : P(x)\}$$

This represents:

"The set of all x such that x satisfies $P(x)$."

where $P(x)$ is a statement about x.

Example: $\mathbb{R}^+ = \{x \mid x \text{ is a positive real numbers}\}$

$\mathbb{R}_0^+ = \{x \mid x \text{ is a non-negative real numbers}\}$

$\mathbb{R}^* = \{x : x \text{ is a non-zero real numbers}\}$

Defn: Empty set is a set that has no elements.

Notation: $\emptyset = \{\}$

$\emptyset$ means empty set.

Defn: A set that contains only one element is called a singleton.

1.1.1 Membership and Equality

Defn: Membership and Equality are fundemental to set theory.

- $x \in A$ if x is an element of A.
- $A = B$ if sets A and B contain precisely the same element.

Both of the above relations may be negated.

- $x \notin A$ if x is not an element of A;
- $A \neq B$ if atleast one element of A is not a member of B, or vice-versa.

Example: (sets of prime factors)
(1.1)

Define sets

$$A = \{p : p \text{ is a prime factor of } 6\} = \{2, 3\}$$

$$B = \{q : q \text{ is a prime factor of } 10\} = \{2, 5\}$$

1 is not a prime number so

$$1 \notin A \quad \text{and} \quad 1 \notin B.$$

Now A has atleast one element namely 3 that doesn't belong to B. Hence

$$A \neq B.$$

Define

$$C = \{p : p \text{ is a prime factor of } 20\} = \{2, 2, 5\} = \{2, 5\}$$

Here

$$C = B.$$

Note: sets ignore repeat elements. This is an inevitable consequence of our definitions. The proof is given below:

proof: Suppose

$$\{2,2,5\} \neq \{2,5\}$$

Then applying the above definitions would mean that one of these sets has an element which doesn't belong to the other and this is not the case. So

$$\{2,2,5\} = \{2,5\}$$

In view of this, it is correct to say:

"10 and 20 have the same set of prime factors"

But 10 and 20 do not have the same prime factorization as that takes into account multiplicity, of each prime.

(Fundemental Theorem of Arithmetic)

1.1.2 Subsets

Defn: Also known as inclusion.
We say A is a subset of another set B, if every element of A is also an element of B.

$$\text{if } x \in A \text{ then } x \in B$$

Notation $A \subseteq B$ represents A is a subset of B.

Note: Every set is a subset of itself: $A \subseteq A$.

Subset relation may be negated.

Defn: $A \not\subseteq B$ means there exists an element of A that doesn't belong to B. i.e.

$$x \in A \text{ and } x \notin B$$

Defn: Proper subset means every element of A belongs to B but there is some element of B not in A. i.e.

$$A \subseteq B \text{ and } A \neq B$$

Here A is called proper subset of B

Notation: $A \subset B$ means A is a proper subset of B.

Theorem: The empty set is the subset of every set i.e.

$$\emptyset \subseteq A$$

for any arbitrary set A.

proof: (by contradiction):

Suppose that

$$\emptyset \not\subseteq A.$$

This would mean: $\exists x$ such that

$$x \in \emptyset \text{ and } x \notin A$$

But $\emptyset$ has no elements: contradiction.
Therefore it must be that

$$\emptyset \subseteq A.$$

Notation: Very common to define new sets as a subset of "old" ones. This leads to a third notation for sets:

$$\{x \in X \mid P(x)\}$$

where X is is some predefined set.

Example: $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$

$\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$

$\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$

Notation: A fourth notation where belong to predefined set X appears as part of the defining property:

$$\{E(x) \mid x \in X\}$$

where $E(x)$ is an expression for x.

Example: $\mathbb{E} = \{2n \mid n \in \mathbb{N}\}$

$= \{2, 4, 6, 8, 10, \ldots\}$

= set of all ever natural numbers defined as subset of $\mathbb{N}$.

The definition of $\mathbb{E}$ could have been the following:

$$\mathbb{E} = \{n \mid n \in \mathbb{N} \text{ and } n = 2m \text{ for some } m \in \mathbb{N}\}$$

Example: (1.2) The following are the subsets of $\mathbb{R}$.

Let $a, b \in \mathbb{R}$ with $a < b$. Then:

$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$ — open, finite

$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ — closed, finite

$[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\}$ — half open/closed, finite

$(a,b] = \{x \in \mathbb{R} \mid a < x \leq b\}$ — half open/closed, finite

$(a,\infty) = \{x \in \mathbb{R} \mid a < x\}$ — open, infinite

$(-\infty,a) = \{x \in \mathbb{R} \mid a < x\}$ — open, infinite

$[a,\infty) = \{x \in \mathbb{R} \mid a \leq x\}$ — closed, infinite

$(-\infty,a] = \{x \in \mathbb{R} \mid a \leq x\}$ — closed, infinite

$(-\infty,\infty) = \mathbb{R}$ ... open and closed, infinite.

Remarks: (1.2)

1) The description of "finite" and infinite refers to the length of the interval, not the number of points it contains.

All intervals contain infinitely many points

2) $\pm\infty$ are not real numbers; i.e. not elements of set $\mathbb{R}$.
We do not allow intervals of form $(a, \infty]$ and such.

3) Intervals such as $[a, \infty)$ and $(-\infty, \infty)$ are referred to as closed.

There is a "standard routine" to show one set is a subset of another.

To show $A \subseteq B$, verify that every element of A is also an element of B. i.e. Show that

if $x \in A$ then $x \in B$.

Example (1.3) (Standard routine for subsets):
Let $A = \{n^2 \mid n \in \mathbb{E}\}$

Claim: $A \subseteq \mathbb{E}$

proof: Suppose $a \in A \Rightarrow a = n^2$ for some $n \in \mathbb{E}$

$n \in \mathbb{E}$ by defn of $A \Rightarrow n = 2m$ for some $m \in \mathbb{N}$

We have:

$$n^2 = (2m)^2 = 4m^2$$
$$= 2(2m^2)$$
$$= 2k \quad (\text{let } k = 2m^2)$$

$2m^2 \in \mathbb{N}$ as $m^2 \in \mathbb{N}$ and $2 \in \mathbb{N}$ so $a = n^2 = 2k \in \mathbb{E}$

So every element of A is also an element of $\mathbb{E}$. Hence

$$A \subseteq \mathbb{E}$$

Also $A \subset \mathbb{E}$ since $A \neq \mathbb{E}$ ∎

1.1.3 Intersections

Defn: The intersection of two sets A and B consists of all the elements A and B have in common. Thus:

Notation: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

Example: $\{1, 2, 0\} \cap \{1, 2, 3\} = \{1, 2\}$

$\mathbb{R}^* \cap \mathbb{R}_0^+ = \mathbb{R}^+$

$(0, 2] \cap [1, 3) = [1, 2]$

Note: $A \cap B \subseteq A$ and $A \cap B \subseteq B$

In fact, $A \cap B$ is the "largest" subset of A and B by which we mean that if $C \subseteq A$ and $C \subseteq B$ then $C \subseteq A \cap B$.

proof: Suppose $x \in C$.

$C \subseteq A$ and $x \in C \Rightarrow x \in A$
$C \subseteq B$ and $x \in C \Rightarrow x \in B$.
Therefore $x \in A$ and $x \in B \Rightarrow x \in A \cap B$
$\Rightarrow C \subseteq A \cap B$. ∎

Defn: We say A and B are <u>disjoint</u> if $A \cap B = \emptyset$

Example: $\{0,1\} \cap \{2,3\} = \emptyset$

$[0,1) \cap (1,2] = \emptyset$

1.1.4 Unions

Defn: The <u>union</u> of two sets A and B consists of all elements of A together with all elements of B.

Notation $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

For example:

$\{0,1,2\} \cup \{1,2,3\} = \{0,1,2,3\}$

$\mathbb{R}^+ \cup \{0\} = \mathbb{R}^+_0$

$(0,2] \cup [1,3) = (0,3)$

Note: $A \subseteq A \cup B$ and $B \subseteq A \cup B$

$A \cup B$ is the smallest set containing both A and B as subsets by which we mean:

if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$

proof: Suppose $x \subseteq A \cup B$

$x \subseteq A \cup B \Rightarrow x \subseteq A$ or $x \subseteq B$

$\Rightarrow x \subseteq C$ or $x \subseteq C$

$\Rightarrow x \subseteq C$

Hence $x \subseteq A \cup B \Rightarrow x \subseteq C$. Therefore

$A \cup B \subseteq C$

■

Defn: If A and B are <u>disjoint</u>, then $A \cup B$ is the <u>disjoint union</u>.

Example: $\{0,1\} \cup \{2,3\} = \{0,1,2,3\}$

↳ disjoint union as $\{0,1\} \cap \{2,3\} = \emptyset$.

Remark (1.4) We can take intersections and unions of infinitely many sets; as long as we're careful, this should not cause problems

Example: let $A_1, A_2, A_3, \ldots$ be sets.

$$I = A_1 \cap A_2 \cap A_3 \cap \ldots = \bigcap_{n \in \mathbb{N}} A_n$$

$$U = A_1 \cup A_2 \cup A_3 \cup \ldots = \bigcup_{n \in \mathbb{N}} A_n$$

$a \in U$ iff $a \in A_n$ for some $n \in \mathbb{N}$

$a \in I$ iff $a \in A_n$ for all $n \in \mathbb{N}$

1.1.5 Set difference

Defn: For any sets A and B, the *set difference* or *relative complement* consists of all elements of A that are not in B.

Notation: $A \setminus B = \{x \in A \mid x \notin B\}$

Example: $\{0,1,2\} \setminus \{1,2,3\} = \{0\}$

$\mathbb{Z} \setminus \mathbb{N} = \{0, -1, -2, \ldots\}$

$(0,2] \setminus [1,3) = (0,1)$

Note: $A \setminus B \subseteq A$

if $A \cap B = \emptyset$ then $A \setminus B = \emptyset$ and $\emptyset \subseteq A$.

1.1.6 Power Sets:

Defn: The *power set of A* denoted $\mathcal{P}(A)$ is the set of all subsets of A:

Notation $\mathcal{P}(A) = \{B \mid B \subseteq A\}$

Example: $\mathcal{P}\{1,2,3\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$\mathcal{P}(\emptyset) = \{\emptyset\}$

Remark (1.5) In the example above, A had 3 elements, i.e.

$$|A| = 3$$

and the number of elements in $\mathcal{P}(A)$ was

$$|\mathcal{P}(A)| = 2^3 = 8$$

So the <u>formula</u> for the <u>number of elements</u> in the <u>power set</u> is:

$\forall$ sets A, if $|A| = N$ then $|\mathcal{P}(A)| = 2^N$

proof (by induction): For $N = 0$ (base case):

$|A| = 0 \Rightarrow A = \emptyset$

$\mathcal{P}(\emptyset) = \{\emptyset\} \Rightarrow |\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0$

Assume property is true for $N=k$

$|A|=k \Rightarrow |\mathcal{P}(A)| = 2^k$ (inductive hypothesis)

Proving that if property is true for $N=k$, then the property is true for $N=k+1$:

Suppose $|A|=k+1 \Rightarrow A = \{a_1, a_2, a_3, \ldots a_{k+1}\}$

$\mathcal{P}(A) = \{N \mid N \subseteq A\}$

$= \{N \mid N \subseteq \{a_1, a_2, a_3, \ldots a_{k+1}\}$

Suppose $B = \{a_1, a_2, a_3, \ldots a_k\}$. Then
$\mathcal{P}(B) = \{N \mid N \subseteq \{a_1, a_2, a_3, \ldots a_k\}$

from the inductive hypothesis,
$|B| = 2^k$,

Any subset of A contains a_{k+1} or it does not contain a_{k+1}.

If a subset of A does not contain a_{k+1}, then it is a subset of B and $|\mathcal{P}(B)| = 2^k$
$\Rightarrow$ There are 2^k subsets of A not containing a_{k+1}

If a subset of A contains a_{K+1}, then that subset is formed by including K+1 in one of 2^K subsets of B.
As a_{K+1} was inserted into each subset of B, then there are 2^K subsets containing a_{K+1}

We have shown that A has 2^K subsets containing a_{K+1} and another 2^K subsets not containing a_{K+1}.

Therefore the total number of subsets is

$$2^K + 2^K = 2(2^K) = 2^{K+1}$$

A has 2^{K+1} subsets so $|\mathcal{P}(A)| = 2^{K+1}$

Therefore from induction, if $|A| = N$, then

$$|\mathcal{P}(A)| = 2^N$$

Example (1.4) (Power sets and probability):
Power set occur naturally in probability theory.

To take a very simple example, if we roll a very standard die, then set of all possible outcomes is

$$A = \{1, 2, 3, 4, 5, 6\}$$

which is referred to as the sample space. However we may want to consider certain types of result like the probability of "rolling an even number." constitute the subset $\{2, 4, 6\}$ which is referred to as an event. The powerset $\mathcal{P}(A)$ may therefore be interpreted as the set of all possible dice rolling events including the no-roll event which corresponds to $\emptyset$.

1.1.7 Complements

Defn: Informally, complement is the set of all things not in A.

This defn only makes sense if we've previously agreed to work inside some bigger set.

$$A^c = \{x \in X \mid x \notin A\}$$

Note $A^c = X \setminus A$

Example: If $\mathbb{R}$ = real numbers and $\mathbb{Q}$ = rational numbers, then

$\mathbb{Q}^c = \mathbb{R} \setminus \mathbb{Q}$ = set of all irrational numbers.

1.1.8 Cartesian (or direct) products

Defn: If A and B are two sets then the set of all ordered pairs (a,b) with $a \in A$ and $b \in B$:

$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

Example: $\{0,1,2\} \times \{1,2,3\} = \{(0,1), (0,2), (0,3), (1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$

Since $x, y \in \mathbb{R}$, the cartesian plane itself can be presented as the cartesian product $\mathbb{R} \times \mathbb{R}$, usually abbreviated as $\mathbb{R}^2$

Note: $(a,b) \neq (b,a)$ unless $a=b$.

↳ order is important!

$(a,b) = (c,d)$ iff $a=c$ and $b=d$.

Remark: (rigorous definition of ordered pair):
(1.6)

Ordered pair can be defined precisely as follows:

$$(a,b) = \{\{a\}, \{a,b\}\}$$

Thus $(a,b) \in \mathcal{P}(A \cup B)$.

Every element of $A \times B$ is an element of $\mathcal{P}(A \cup B)$ which means by subset property:

$$A \times B \subset \mathcal{P}(A \times B)$$

This definition also allows us to deduce the rules:
For suppose

$$\{\{a\}, \{a,b\}\} = \{\{c\}, \{c,d\}\} \qquad (*)$$

If $a \neq b$ then from principle of equality of sets,

$\{a\} = \{c\}$ and $\{a,b\} = \{c,d\}$

and then $a=c$ and $b=d$.

If $a=b$ then the $(*)$ collapses to

$$\{\{a\}\} = \{\{c\}, \{c,d\}\}$$

and principle of equality implies $d=c=a$; hence $a=c$ and $b=d$ once again.

Defn: We can extend cartesian product to three (or more sets) A, B, C by defining:

$$A \times B \times C = \{(a,b,c) : a \in A,\ b \in B,\ c \in C\}$$

where (a,b,c) is an ordered triple.

Again if we take $A = B = C = \mathbb{R}$, then we end up with $\mathbb{R}^3$, the cartesian space with co-ordinates (x,y,z).

1.1.9 Principle of Mutual Containment

Defn: if A and B are two sets and we can show that $A \subseteq B$ and $B \subseteq A$, then $A = B$. Thus:

$\forall$ sets A and B, $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$.

Proofs often adopt the following template:

To show $A = B$

- Let $x \in A$ and show $x \in B$. Conclude $A \subseteq B$
- Conversely, let $y \in B$ and show $y \in A \Rightarrow B \subseteq A$
- Conclude $A = B$

Example: (principle of mutual containment):
(1.5)

Let $A = \{n-m : m,n \in \mathbb{Z}\}$. Show that $A = \mathbb{Z}$

($\subseteq$): $m \in \mathbb{N}$ $n \in \mathbb{N}$ so $n-m \in \mathbb{Z}$

$n-m \in A \Rightarrow n-m \in \mathbb{Z}$

Hence $A \subseteq \mathbb{Z}$

($\supseteq$): Suppose $a \in \mathbb{Z}$. Then there are three cases to consider:

- if $a > 0$, then $a = n-m$ where $n = a+1$ and $m = 1$ (for example); so $a \in A$
- if $a = 0$, then $a = 1-1$ (for example) so $a \in A$
- if $a < 0$ then $a = n-m$ where $n = 1$ and $m = 1-a$, so $a \in A$. (for example)

Hence $a \in A$. Therefore $\mathbb{Z} \in A$.

It follows from principle of mutual containment that

$$A = \mathbb{Z}$$

1.1.10 Basic laws of set theory.

- The "commutative law of intersection":

$$A \cap B = B \cap A$$

- The "commutative law of union":

$$A \cup B = B \cup A$$

- The "associative law of intersection":

$$A \cap (B \cap C) = (A \cap B) \cap C$$

- The "associative law of union":

$$A \cup (B \cup C) = (A \cup B) \cup C$$

- The "first distributive law":

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

- The "second distributive law":

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

- "De Morgan's first law":

$$(A \cup B)^c = A^c \cap B^c$$

- "De Morgan's second law":

$$(A \cap B)^c = A^c \cup B^c$$

- The "double complement law":

$$(A^c)^c = A$$

Example: (First distributive law):
(1.6)

Proof of first distributive law using principle of mutual containment

$$x \in A \cap (B \cup C) \iff x \in A \text{ and } x \in B \cup C$$

$$\iff x \in A \text{ and } (x \in B \text{ or } x \in C)$$

$$\iff (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)$$

$$\iff x \in A \cap B \text{ or } x \in A \cap C$$

$$\iff x \in (A \cap B) \cup (A \cap C)$$

Note that all implications shown in previous example are reversible

This shows that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ showing that

$A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ have the exact same elements Hence

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

■

Example: (1.7) (Double Complement law):
This is the proof for double complement law:

Suppose $A \subseteq X$.
By defn of complement:

$$x \in (A^c)^c \iff x \notin A^c \qquad (*1)$$

Since to be an element of A. is to not be an element of A^c and
to not be an element of A^c is "not not be" an element of A; in otherwords be an element of A.

Therefore

$$x \notin A^c \iff x \in A \qquad (*2)$$

Putting $(*1)$ and $(*2)$ together gives:

$$x \in (A^c)^c \iff x \in A.$$

Hence A and A^c have precisely the same elements

1.2 Functions

Defn (1.1): (Functions):
A function $f: A \to B$ consists of three things:

- A set A called domain
- Another set B called co-domain.
  Its allowed that $B = A$.
- A rule f which describes unambiguously how to associate each element $a \in A$ a unique element $f(a) \in B$.

Notation: $f: A \to B$ represents a function from set A to B.

Remark (1.9) (Functions):

1) The notation $A \xrightarrow{f} B$ is ocassionally used.

2) The terminology map, mapping or transformation is used.

3) The notation $a \mapsto f(a)$ is often used when defining the rule f.
for example: the rule $f(x) = x^2$ for a function $f: \mathbb{R} \to \mathbb{R}$ is also denoted $x \mapsto x^2$.

4) If $a \in A$, then $f(a)$ is sometimes called the value of f at a, and a itself is rather quaintly the argument for this value.

$a \in A$ is also commonly referred to as the input, or independant variable

$f(a) \in B$ is commonly referred to as the output or, dependant variable.

Example: (square root functions):
(1.8)
The rule:
"take the square root of a non-negative number x"

is ambiguous, since if $x > 0$, there are 2 possibilities: $\pm\sqrt{x}$.
So this rule does not define a function.

However, if we agree to choose the nonnegative square root function denoted $\sqrt{x}$, then this is unambiguous and therefore defines the following functions:

$$f: \mathbb{R}_0^+ \to \mathbb{R} : x \mapsto \sqrt{x}$$

domain ↑ codomain ↑

1.2.1 Principle of Equality of Functions:

Defn: We say that functions $f: A \to B$ and $g: C \to D$ are equal if:

- $A = C$; i.e. they have the same domain
- $B = D$; i.e. they have the same codomain
- $f = g$; they have the same rule.

Having the same rule means:

$$f(a) = g(a) \quad \forall\, a \in A$$

Notation: $(f : A \to B) = (g : C \to D)$

↳ This is pretty clunky we use:

$$f = g$$

1.2.2 Images:

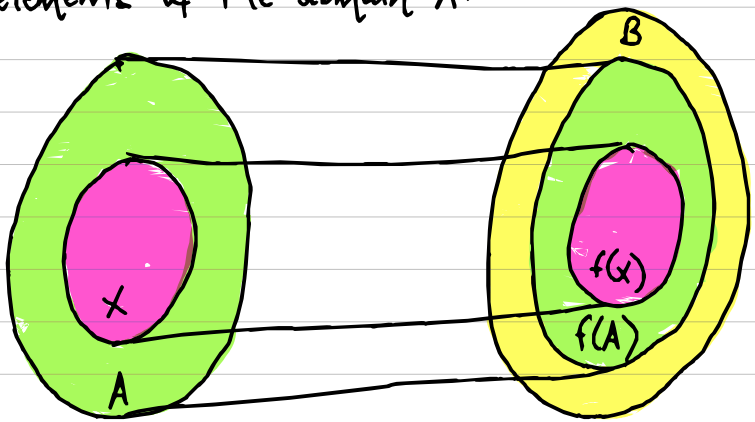
Given a function $f : A \to B$ and an element $a \in A$, $\underline{f(a) \in B}$ is sometimes referred as image of A under f.

Defn (1.2): (Image)
Suppose $f : A \to B$ is a function. If $\underline{X \subseteq A}$ then the $\underline{\text{image of } X \text{ under } f}$ is the subset $\underline{f(x) \subseteq B}$ defined

$$f(X) = \{ f(x) \mid x \in X \}$$

In particular, $f(A)$ is called the $\underline{\text{image of } f}$, often denoted $\underline{\text{im}(f)}$

$\mathrm{Im}(f)$ is the set of values in the codomain B that the function takes as we plug in all the elements of the domain A.



Remarks (1.10)

(image)

The codomain can be much larger than the image.

Example:

$f: \mathbb{R} \to \mathbb{R} : f(x) = 0$ is defined $\forall x \in \mathbb{R}$ and

$$\mathrm{im}(f) = f(\mathbb{R}) = \{0\}$$

Thus the function $f: A \to B$ is strictly speaking different to the function $f: A \to f(A)$

If $X \subset A$ (proper subset), it is nevertheless possible for $f(X) = f(A)$.

Example: $f(x) = c$ for all $c \in \mathbb{R}$.

Example: (square root function; images).
(1.9)

$$f : \mathbb{R}_0^+ \to \mathbb{R} : x \mapsto \sqrt{x}$$

Codomain of f is clearly $\mathbb{R}$. Image of f is $\mathbb{R}_0^+$

(Since none of its values is negative, and every non-negative real number y is the square root of a non-negative real number x, namely $x = y^2$).

Now, here are images of certain subsets of $\mathbb{R}_0^+$ under f.

$$f(\mathbb{N}) = \{1, \sqrt{2}, \sqrt{3}, 2, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, 3, \ldots\}$$

$$f(a,b) = (\sqrt{a}, \sqrt{b}) \quad \text{for } 0 \leq a \leq b$$

$$f[a,\infty) = [\sqrt{a}, \infty) \quad \text{for } a \geq 0.$$

1.2.3 One-to-one and Onto functions:

Defn: (1.3) (One-to-one and/or onto)
Suppose $f: A \to B$.

- We say that f is one to one (injective), often abbreviated 1-1, if distinct elements of the domain A are sent to distinct elements of the domain B.
  More precisely:

> If $x, y \in A$ with $x \neq y$ then $f(x) \neq f(y)$

In practise, we use the logically equivalent contrapositive statement:

> If $x, y \in A$ satisfy $f(x) = f(y)$ then $x = y$.

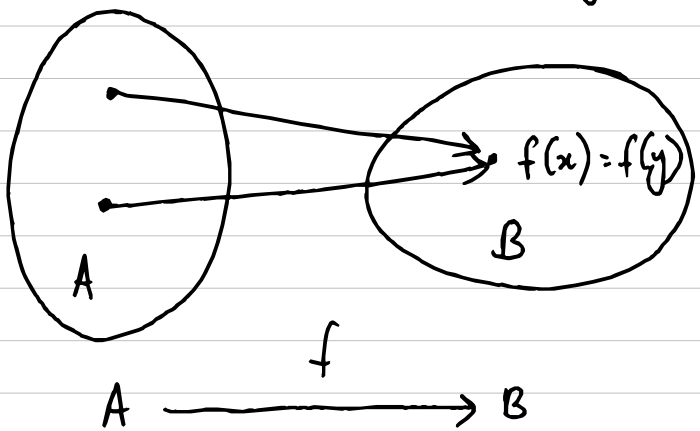
- We say that f is onto (surjective) if every element of B comes from some element of A, via f. More precisely:

> Given any $b \in B$, there exists some $a \in A$ such that $f(a) = B$.

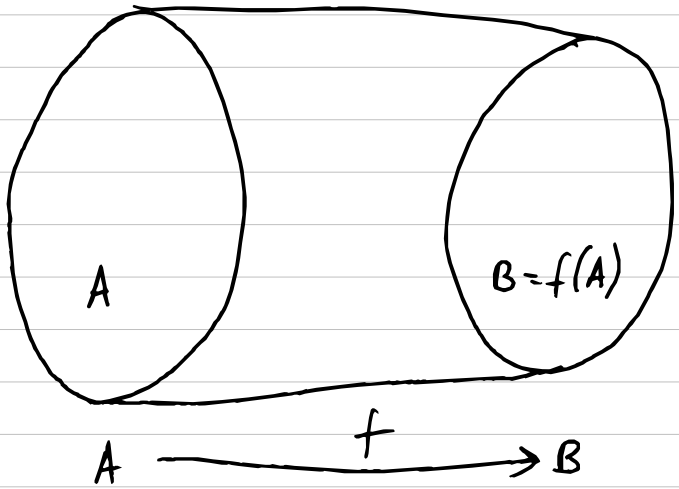
or

> $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

The element a isn't necessarily unique.



Not one-to-one.



onto function

Example (1.10) (Increasing and decreasing functions.)
Suppose $f: A \to B$, where A and $B \subseteq \mathbb{R}$.

- f is <u>increasing</u> if $x < y \Rightarrow f(x) < f(y)$
- f is <u>decreasing</u> if $x < y \Rightarrow f(x) > f(y)$.

In either case, f is one to one

proof: (using original defn):

if f is one to one then $\forall x, y \in A,\ x \neq y \Rightarrow f(x) \neq f(y)$.

$x \neq y \Rightarrow x < y$ or $x > y$.

if $x<y$ or $x>y$, in which case, $f(x)<f(y)$ or $f(x)>f(y)$, hence $f(x) \neq f(y)$.

■

If a function is not one-to-one or onto, then we may be able to

- salvage the injectivity by restricting the domain
- salvage the surjectivity by reducing size of codomain.

without changing the rule.

Example: (1.11) (Injective and Surjective functions.):

Consider $f: \mathbb{R} \to \mathbb{R}$ defined $f(x) = x^2$.
Then f is not one to one:

$$f(-1) = f(1) = 1.$$

Furthermore f is not onto. $\exists$ no real numb x with $f(x) = -1$.

Now, if we restrict the domain of f to $\mathbb{R}_0^+$ we obtain a new function

$$f: \mathbb{R}_0^+ \to \mathbb{R}$$

defined by the same rule, but is now one to one.

We will verify this using the "standard routine"

Suppose $f(a) = f(b)$ for $a, b \in \mathbb{R}_0^+$; thus:

$$a^2 = b^2,$$

$$\Rightarrow \quad a^2 - b^2 = 0 \Rightarrow (a-b)(a+b) = 0$$

Hence either $a-b=0$ or $a+b=0$, so $a=b$ or $a=-b$

$a=-b$ is impossible since $a, b \in \mathbb{R}_0^+$ and a is non-negative.

Therefore $a=b$

On the otherhand, if we reduce the codomain of f from $\mathbb{R}$ to the image $f(\mathbb{R})$, we immediately obtain a surjection

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

What is $f(\mathbb{R})$?
Since squares of real numbers are non-negative, we have

$$f(\mathbb{R}) \subseteq \mathbb{R}_0^+$$

For every $y \in \mathbb{R}_0^+$, $\exists\, x \in \mathbb{R}$ such that $y = f(x)$ where $x = \sqrt{y} \in \mathbb{R}$, so $y \in f(\mathbb{R})$. So,

$$\mathbb{R}_+^0 \subseteq f(\mathbb{R}).$$

Thus $\mathbb{R}_+^0 = f(\mathbb{R})$ by mutual containment.
So the function

$$f: \mathbb{R} \to \mathbb{R}_0^+$$

is onto.

Putting both modifications, produces function,

$$f: \mathbb{R}_0^+ \to \mathbb{R}_0^+ \quad x \mapsto x^2$$

which is both one-to-one and onto.

Example (1.12) (Functions of Cartesian Product):
For a slightly different kind of function, consider

$$f: \mathbb{N} \times \mathbb{N} \to \mathbb{Z}:$$
$$f(m,n) = n - m \qquad \forall\, m,n \in \mathbb{N}$$

Every integer can be written as a difference of 2 natural numbers. Therefore, $\forall\, f(m,n) \in \mathbb{Z}$ $\exists\, (m,n) \in \mathbb{Z}$ s.t $f(m,n) = n-m$ Therefore f is onto.

However, $f(1,1) = 0 = f(2,2)$ and $(1,1) \neq (2,2)$ shows f is not one-to-one.

1.2.4 Bijections and Inverse Functions:

If a function is one-to-one and onto, then it pairs up the elements of the domain and co-domain.
This means there is another function going the other way.
↳ the inverse function.

Defn: (1.4) (Bijection and inverse function)

Suppose $f: A \to B$ is a function.

- We say that f is bijective (one-to-one correspondance) if f is one to one and onto
Thus combining two parts of defn 1.3,

f is bijective if and only if the following condition holds:

> for every $b \in B$, $\exists$ a unique $a \in A$ such that $f(a) = b$

- The unique element $a \in A$ such that $f(a)=b$ is denoted $f^{-1}(b)$.

The rule "associate to $b \in B$, the element"

$$f^{-1}(b) \in A$$

then defines the function:

$$f^{-1}: B \to A$$
$$f^{-1}(b) = a$$

called the inverse function.
By definition, it satisfies the property:

$$f(f^{-1}(b)) = b \quad \forall\, b \in B.$$

Thus "f undoes f^{-1}"

Note: If we take $b = f(a)$ in defn (1.4), we see immediately that

$$f^{-1}(f(a)) = f \quad \forall\, a \in A.$$

Thus "f^{-1} undoes f"

Proposition (1.1): (Inverse of a bijection):

i) The inverse of a bijection $f: A \to B$ is also a bijection.

(ii) In this situation, the inverse of $f^{-1}: B \to A$ is $f: A \to B$, i.e. $(f^{-1})^{-1} = f$

proof: For notational convenience, denote $g = f^{-1}$ so $g: B \to A$.

(i) Verifying g is one-to-one using "standard routine"

Suppose

$$g(b_1) = g(b_2) \quad \text{for } b_1, b_2 \in B.$$

Applying f to both sides;

$$f(g(b_1)) = f(g(b_2))$$

Thus

$$b_1 = b_2$$

as required, so g is one to one.

Now verify that g is onto.
Suppose $a \in A$. Then we have $a = g(b)$, where $b = f(a)$.
So $\forall\, a \in A, \exists\, b \in B$ s.t $a = g(b)$, namely $b = f(a)$.

It follows by defn that g is a bijection.

(ii) g is a bijection, so it has inverse:

$$g^{-1}: A \to B$$

which satisfies

$$g(g^{-1}(a)) = a \qquad \forall\, a \in A$$

Applying f to both sides gives us

$$f(g(g^{-1}(a))) = f(a)$$

$$\Rightarrow \quad g^{-1}(a) = f(a) \qquad \forall\, a \in A.$$

Therefore $g^{-1} = f$ by principle of equality of fns. ■

Example: (Linear bijections):
(1.3)

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

$$f(x) = ax + b \quad , a, b \in \mathbb{R}, a \neq 0.$$

f is a linear or more precisely an affine function.

f is one-to-one because if $f(x) = f(y)$,

$$a(x) + b = a(y) + b \qquad \text{cancelling } b$$

$$\Rightarrow$$

$$x = y \qquad \text{dividing by } a \neq 0$$

as required. So f is one-to-one.

Furthermore, f is onto. As

$\forall y \in \mathbb{R}, \exists x \in \mathbb{R}$ namely $x = \frac{y-b}{a}$ s.t

$$f(x) = f\left(\frac{y-b}{a}\right) = \frac{a(y-b)}{a} + b$$

$$= y$$

x can be found by solving

$$y = ax + b$$

for x, i.e.

$$ax = y - b \Rightarrow x = \frac{y-b}{a}.$$

Thus $y = f(x)$ with x as above.

So f is a bijection, and therefore has an inverse

$$f^{-1}: \mathbb{R} \to \mathbb{R}$$

which by defn has rule:

$$f^{-1}(y) = \frac{y-b}{a} \quad \forall\, y \in \mathbb{R}.$$

□

Defn: (1.5) (Invertible function):
A function $f: A \to B$ is <u>invertible</u> if there exists a function $g: B \to A$ such that:

$$g(f(a)) = a, \qquad (*)$$
$$f(g(b)) = b$$

$\forall\, a \in A$ and $\forall\, b \in B$.

Remark: (1.15) 1) A function satisfying both equations in defn 1.5, <u>is necessarily unique</u>

For if <u>h is another function</u> then it follows from the equations in defn 1.5 (applied to both h and g) that for all $b \in B$,

$$h(b) = h(f(g(b))) = g(b)$$

Hence $h = g$ by Principle of Equality of Functions

2) By defn the function g is also invertible if it satisfies $(*)$.

Proposition: (Invertible functions are bijections): (1.2)

Suppose $f: A \to B$ is invertible. Then f is a bijection and $f^{-1} = g$ where g is unique fn satisfying equations in defn 1.5.

proof: Showing that f is one-to-one using "standard routine": suppose:

$$f(a_1) = f(a_2) \quad \forall a_1, a_2 \in A.$$

Then applying g to both sides:

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

$$\Rightarrow \quad a_1 = a_2.$$

Now to show f is onto.

$\forall b \in B$, $\exists$ an $a \in A$ namely $a = g(b)$ s.t

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

It follows that f is a bijection with inverse:

$$f^{-1}: B \to A.$$

Comparing f^{-1} to g and noting uniqueness of g,

$$f^{-1} = g$$

■

Remark: (1.16) (Left and right invertible functions)
Close inspection of proof of proposition 1.2 shows that f is one to one only if we use the first eqn in defn 1.5, where as we use the second equation to show f is onto.
When we want to distinguish between those two equations, we say that f is <u>left-invertible</u> or <u>right-invertible</u> respectively.

It possible to define functions such that only <u>one of the equations</u> in defn 1.5 is satisfied.

Example: $f: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $f(n) = (n, n)$

$g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $g(m, n) = m$,

Then for all $n \in \mathbb{N}$, we have

$$g(f(n)) = g(n,n) = n$$

So f is left invertible. g is the left-inverse.

However for all $(m,n) \in \mathbb{N} \times \mathbb{N}$ we have:

$$f(g(m,n)) = f(m) = (m,m)$$

So g is not a right-inverse (or equivalently, f is not a left inverse for g).

Unlike inverse functions, left inverse/right-inverse need not be unique.
For example if f is the function defined in the previous paragraph then

$$h: \mathbb{N} \times \mathbb{N} \to \mathbb{N};\ (m,n) \mapsto n$$

is another left inverse of f.

It turns out that left-invertibility is equivalent to being one-to-one

right-invertibility is equivalent to being onto.

Example 1.14: (Set complement as a function on power set): Let A be any set and define

$$f: \mathcal{P}(A) \to \mathcal{P}(B) \text{ by rule}$$

$$f(X) = X^C$$

for all sets $X \in \mathcal{P}(A)$.

By double complement law;

$$f(f(X)) = f(X^C) = (X^C)^C = X$$

Hence f is invertible and it follows from proposition 1.2 that

f is a bijection with $f^{-1} = f$.

1.2.5 Composition of Functions:

Defn (1.6) (composition)

Suppose $f: A \to B$ and $g: B \to C$ are functions. Then the composition is the function denoted by $g \circ f: A \to C$ whose is defined:

$$(g \circ f)(a) = g(f(a)) \quad \forall\, a \in A$$

Thus $g \circ f$ is the rule "do f, then do g"

Remarks (1.17): (Elementary Properties of Composition):

1) We can only compose two functions if the codomain of the first is the same as (or more generally as a subset of) the domain of the second function.
Otherwise the rule $g \circ f$ does not make sense.

2) Composition of functions is associative:

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

for any functions:

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

In other words for all $a \in A$, we have

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

and ultimately:

$$h(g(f(a))) = h(g(f(a)))$$

3) Having established associativity, we can write:

$$h \circ g \circ f$$

without any danger of ambiguity.

4) Composition of functions <u>isn't commutative</u>:

$$g \circ f \neq f \circ g$$

Indeed in general composition $f \circ g$ won't make sense unless $A = B$.
However even in case, two functions $f, g : A \to A$, won't in general commute

5) The composition notation allows us to invoke the Principle of equality of functions to "<u>clean up</u>" inverse function composition notation:

$$f \circ f^{-1} = 1_B$$

$$f^{-1} \circ f = 1_A$$

where 1_A $A \to A$ and 1_B $B \to B$ are <u>identity functions</u>

$$1_A(a) = a \qquad 1_B(b) = b.$$

$\forall a \in A,\ b \in B.$

Example: (Function of a function):
(1.15)

Suppose $f, g: \mathbb{R} \to \mathbb{R}$ are given by $f(x) = x^2$ and $g(x) = x+1$.

Then $\forall x \in \mathbb{R}$

$$(g \circ f)(x) = g(x^2) = x^2 + 1.$$

whereas:

$$(f \circ g)(x) = f(x+1) = (x+1)^2$$

For these two functions to be decreed equal, they have to agree for all x, by principle of equality of functions

However $(f \circ g)(1) = 4$ and $(g \circ f)(1) = 2$.

Thus $g \circ f \neq f \circ g$

So this pair does <u>not</u> commute. □

Proposition (1.3): (Composition of bijections):
The composition of injections is injective.
The composition of surjections is surjective.
Therefore the composition of bijections is bijective, and in this case:

$$(g \circ f) = f^{-1} \circ g^{-1}$$

proof: Suppose f and g are injective. Showing $g \circ f$ is injective using the "standard routine":

$$(g \circ f)(x) = (g \circ f)(y)$$

$$\Rightarrow g(f(x)) = g(f(y))$$

$$\Rightarrow f(x) = f(y) \quad \text{because } g \text{ is one to one}$$

$$\Rightarrow x = y \quad \text{because } f \text{ is one to one.}$$

Thus $g \circ f$ is one-to-one.

Now suppose f and g are surjective.
Given $c \in C$. $\exists$ an element $b \in B$ with $g(b) = c$, since g is onto.
Further more, $\exists$ an element $a \in A$ with $f(a) = b$ since f is onto.
Hence

$$c = g(b) = g(f(a)) = (g \circ f)(a)$$

Thus $g \circ f$ is onto.

It follows immediately that if f, g are bijective Then so is $g \circ f$.

The inverse function $(g \circ f)^{-1} : C \to A$ is characterized by the condition that its value at any point $c \in C$ is the unique element A such that $(g \circ f)(a) = c \Rightarrow g(f(a)) = c$

↳ By $f(f^{-1}(b)) = b, \forall b \in B$, this equation is satisfied if:

$$a = f^{-1}(g^{-1}(c)) = (f^{-1} \circ g^{-1})(c)$$

hence by uniqueness:

$$(g \circ f)^{-1}(c) = (f^{-1} \circ g^{-1})(c) \quad \forall c \in C$$ ☆

* derivation:

$$(g \circ f)(a) = g(f(a)) = c$$

$$\Rightarrow g^{-1}(g(f(a))) = g^{-1}(c)$$

$$\Rightarrow f(a) = g^{-1}(c)$$

$$\Rightarrow f^{-1}(f(a)) = f^{-1}(g^{-1}(c))$$

$$\Rightarrow a = f^{-1}(g^{-1}(c))$$

$$\Rightarrow a = (f^{-1} \circ g^{-1})(c).$$

So $(f^{-1} \circ g^{-1}) : C \to A \; ; \; (f^{-1} \circ g^{-1})(c) = a$

and $(g \circ f)^{-1} : C \to A \; ; \; (g \circ f)^{-1}(c) = a$

By principle of equality of functions:

$$\boxed{(g \circ f)^{-1} = (f^{-1} \circ g^{-1})}$$

which by principle of equality of functions allows us to write:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

■

Example (1.16): (Inverse of composition):
Suppose $h: \mathbb{R} \to \mathbb{R}$ is defined $h(x) = 2x + 5 \ \forall x \in \mathbb{R}$.
and $f: \mathbb{R} \to \mathbb{R}$ $f(x) = 2x$ and $g(x) = x + 5$.
Then

$$h = g \circ f$$

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

$$= g(2x) = 2x + 5$$

f and g are bijections with inverses

$$f^{-1}: \mathbb{R} \to \mathbb{R}; \ f^{-1}(x) = \tfrac{1}{2}x$$

$$g^{-1}: \mathbb{R} \to \mathbb{R}; \ g^{-1}(x) = x - 5$$

Proposition (1.3) tells us that h is a bijection with inverse $h^{-1}: \mathbb{R} \to \mathbb{R}$ defined

$$h^{-1}(x) = (f^{-1} \circ g^{-1})(x) = f^{-1}(g^{-1}(x))$$

$$= f^{-1}(x - 5) = \tfrac{1}{2}(x - 5)$$

□

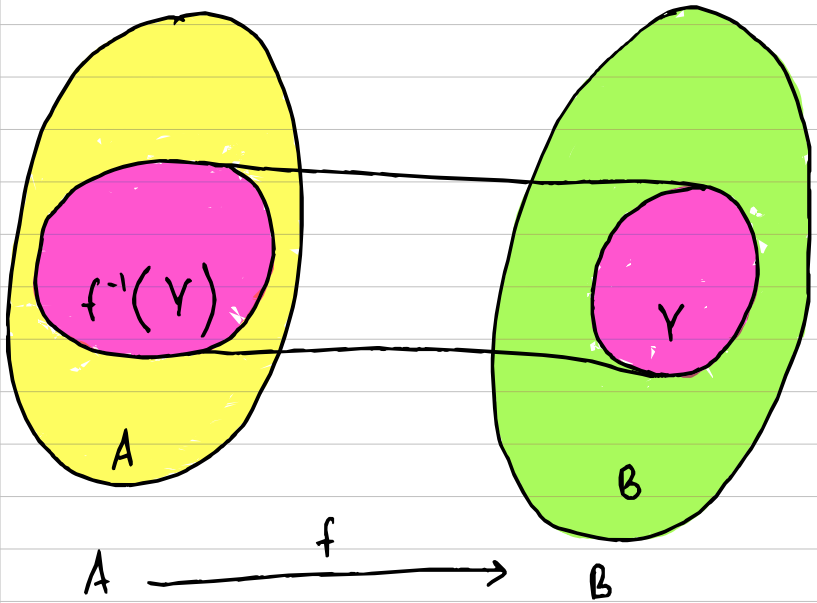
1.2.6 Preimages

Defn (1.7): (Preimage):
Suppose $f: A \to B$ is a function, and $Y \subseteq B$.
Define <u>preimage</u> of Y under f to be the following subset of A:

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

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

↳ a subset of all points of A that map to y.



Remark: (Image and Preimages): (1.18)

By definition, the image of a pre-image is the original subset:

$$f(f^{-1}(Y)) = Y \qquad \forall\, Y \subseteq B$$

due to fact that every x has unique y, function cannot be many to one

However, if $X \subseteq A$ then the preimage of its image clearly contains X but could in fact be larger. So in general we can only say:

$$X \subseteq f^{-1}(f(X))$$

(due to fact that function could be many to one)

Remark: (Fibres of a function): (1.19)

If $Y = \{y\}$ for some $y \in B$, then we usually write

$$f^{-1}(y)$$

rather than $f^{-1}\{y\}$ or $f^{-1}(\{y\})$; thus

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

We refer to this as the fibre of f over y (or particularly in calculus, the level set of f with value y).

Examples: (Preimages):
(1.17) We return to the function

$$f: \mathbb{R} \to \mathbb{R}$$
$$x \mapsto x^2$$

Note that f is not bijective, so there is no inverse $f^{-1}: \mathbb{R} \to \mathbb{R}$

Nevertheless we can use the symbol f^{-1} when dealing with preimages.

1) Here are a few pre-images:

$$f^{-1}(\mathbb{R}) = \mathbb{R}$$

$$f^{-1}(\mathbb{R}_0^+) = \mathbb{R}$$

$$f^{-1}(\mathbb{R}^+) = \mathbb{R}^*$$

$$f^{-1}(a) = \{-a, a\} \text{ for } a > 0$$

$$f^{-1}[0, a) = \{-\sqrt{a}, \sqrt{a}\} \text{ for } a > 0$$

$$f^{-1}[a, b) = (-\sqrt{b}, -\sqrt{a}\,] \cup [\sqrt{a}, b)$$

$$f^{-1}(-\infty\ 0\,] = \{0\}$$

$$f^{-1}(-\infty, 0) = \emptyset$$

↓ since no $a \in \mathbb{R}$ can map to a negative number

2) Here's a <u>counterexample</u> to the statement

$$f^{-1}(f(X)) = X.$$

for all subsets of X of the domain.
In spirit of making counter examples as simple as possible:

let $X = \{1\}$

Then $f(X) = \{1\}$

hence

$$f^{-1}(f(X)) = f^{-1}(1) = \{-1, 1\} \supseteq X$$

On the other hand, if we take preimage first then

$$f(f^{-1}(X)) = f\{-1, 1\} = \{1\} = X$$

as noted in remark 1.18.

□

Example: (Circles as Preimages):
(1.18) Define $f: \mathbb{R} \to \mathbb{R}$;

$$f(x,y) = x^2 + y^2$$

and suppose $k \in \mathbb{R}$

if $k<0$, $f^{-1}(k) = \emptyset$

if $k=0$, $f^{-1}(k) = \{(0,0)\}$

However if $k>0$ and write $k = r^2$ for $r>0$, then the fibre of f over k is:

$$f^{-1}(k) = \{(x,y) : x^2 + y^2 = r^2\}$$

Visualising $\mathbb{R}^2$ as the cartesian plane, we recognise this as the circle of radius r centred at origin $(0,0)$

So in geometry and calculus, fibres of functions are nothing other than what we call level curves (or in higher dimensions, level surfaces). defined by an implicit equation.

1.2.7 Cardinality

Question: What does it mean for sets to have the same size?

For any natural number n, the following set

$$[n] = \{1, 2, \ldots, n\}$$

is finite and has n elements.

Suppose A is a set.
To determine whether A is finite or not, we "count" its elements.
First pick any element of A for convenience call it a_1.
We now pick any element from $A \setminus \{a_1\}$ say a_2.
Now pick from $A \setminus \{a_1, a_2\}$ and so on.
If there exists a natural number $n \in \mathbb{N}$ s.t $A \setminus \{a_1, a_2, \ldots, a_n\} = \emptyset$, then we can agree A is finite, with n elements

$$A = \{a_1, \ldots, a_n\}$$

Now define a function

$$f_A : [n] \to A ;$$

$$f(i) = a_i$$

f_A is clearly onto as $\forall\, a_i \in A \;\exists\, i \in \mathbb{N}$, s.t. $f(i) = a_i$

f_A is clearly one to one, since by construction,

$$a_i = a_j \Rightarrow i = j$$

So f_A is clearly a bijection.
This suggests an elegant way of defining finite sets and number of elements they contain.

Defn: (1.8) A non-empty set is finite if if there exists a bijection $f : [n] \to A$ for some $n \in \mathbb{N}$
The cardinality is then defined:

$$|A| = n$$

We say A is infinite if it is not finite.

Remark: 1.20 The empty set $\emptyset$ does not satisfy our definition for a finite set.
We do not want to decree $\emptyset$ as an infinite set.
So define

$$|\emptyset| = 0$$

Our definition of cardinality has a potential problem:
Could counting the elements in a set in different ways lead to different cardinalities?

More precisely, the procedure for constructing f_A involves involved making choices therefore if applied differently could conceivably produce different values of n.

↳ If this is the case our defn is useless.

To see this cannot happen, suppose we have 2 bijections

$$f:[n]\to A \qquad g:[m]\to A$$

Then the composition

$$F = g\circ f^{-1} : [n]\to[m]$$

is also a bijection by proposition 1.1 and 1.3

Now we have to prove $m=n$.

Proposition (1.4): Suppose $f:[m]\to[n]$

(i) if f is one to one then $m\leq n$

(ii) if f is onto then $m\geq n$.

Therefore if f is a bijection, $m=n$.

proof:

(i) Induction on m,

Let $P(m)$ be the statement:

"$\forall n$, if $[m] \to [n]$ is one-to one then $m \leq n$"

Then $P(1)$ is true since $1 \leq n$ for all $n \in \mathbb{N}$

Assume $P(m)$ is true,

Suppose $[m+1] \to [n]$ is one to one
If $c = f(m+1)$, then restricting f to $[m]$ gives us a new function,

$$g : [m] \to [n] \setminus \{c\}$$

which is also one to one

Now define function $h : [n] \setminus \{c\} \to [n-1]$ by

$$h(x) = \begin{cases} x & \text{if } x < c \\ x-1 & \text{if } x > c \end{cases}$$

h is one to one for if

$$h(r) = h(s)$$

is only possible if $r, s < c$ or $r, s > c$ and in both cases, $r = s$.

The composition

$$h \circ g : [m] \to [n-1]$$

is one-to-one so by inductive hypothesis

$$m \leq n-1$$

Hence $m+1 \leq n$ so $P(m+1)$ is true.

So by principle of induction,

$P(m)$ is true for all m.