# Sets and Maps

Sets are the most basic objects in mathematics.

Basic notation  A set contains elements

"$x$ is an element of $X$", which means the same as "$X$ contains the element $x$" is written "$x \in X$"

"$\subset$" or "$\subseteq$" mean the same: "is a subset of"

Def$^n$ $A \subset B$ means "every element of $A$ is also an element of $B$" This can be written as

$$(A \subset B) \iff (x \in A \Rightarrow x \in B)$$

$\{a\}$ means "the set" containing the single element $a$"

$\{x_1, x_2, x_3\}$ means "the set containing just the 3 elements $x_1, x_2, x_3$"

$:$ means "such that" ($|$ can also be used for "such that")

$X = \{x : x$ is a person born in $1993\}$

$Y = \{x : x$ is a person born in Liverpool in $1993\}$

$Y \subset X$.   Both these are conditional definitions of sets

$\{n \in \mathbb{Z} : 2 | n\}$ is the set of all even integers

$\{n \in \mathbb{N} : n \neq 0 \wedge n \neq 1 \wedge (\overset{p \in \mathbb{N},}{p | n} \Rightarrow p = 1 \vee p = n)\}$ is the set of all prime (natural) numbers

$\phi$ is the empty set.

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

$\cup$ $\quad A \cup B = \{x : x \in A \vee x \in B\}$

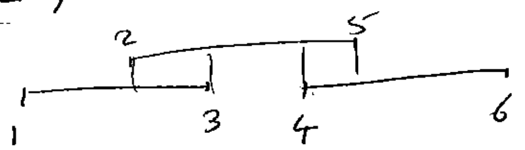
$\cap$ $\quad A \cap B = \{x : x \in A \wedge x \in B\}$

$\setminus$ $\quad A \setminus B = \{x : x \in A \wedge x \notin B\}$

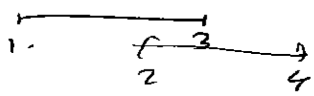
<u>Intervals</u>. $[a,b]$, $[a,b)$ etc.

<u>Examples</u> Write the following as unions of intervals in the simplest possible ways

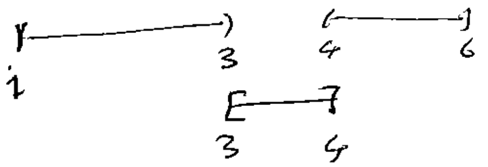
(1) $([1,3] \cup [4,6]) \cap [2,5] = [2,3] \cup [4,5]$



(2) $[1,3] \cup (2,4) = [1,4)$



(3) $([1,3) \cup (4,6]) \cap [3,4] = \phi$



<u>Maps/Functions</u>

A map (or function) $f : X \longrightarrow Y$ means $f$ is a map <u>from</u> the set $X$ <u>to</u> the set $Y$. This means that, for each $x \in X$, $f(x)$ is defined with $f(x) \in Y$. It is <u>not</u> required that every element of $Y$ is of the form $f(x)$.

$X$ is the <u>domain</u> of $f$ and $Y$ is the <u>codomain</u>

Examples of maps/functions $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = 2n$.

$f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f_1(x) = x^2$ $\mathbb{R}$ is the domain and also the codomain

$f_2 : (0, \infty) \longrightarrow \mathbb{R}$ defined by $f_2(x) = 1/x$

$(0,\infty)$ is the domain of $f_2$ and $\mathbb{R}$ is the codomain.

Techically the map (function) $g_1 : \mathbb{R} \longrightarrow [0,\infty)$ defined by $g_1(x) = x^2$ is different from $f_1$ above, because it has a different codomain

$g_2 : (-\infty, 0) \cup (0, \infty) \longrightarrow \mathbb{R}$ defined by $g_2(x) = 1/x$

$g_2$ is techically different from $f_2 : (0,\infty) \longrightarrow \mathbb{R}$ given above, because it has a different domain.

$g : \mathbb{R} \longrightarrow \mathbb{R}$ defined by

$$g(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases}$$

is a map (function)

Composition of functions (maps)

If $f : X \longrightarrow Y$ and $g : Y \to Z$ are functions, then we can define a function $g \circ f : X \longrightarrow Z$ (domain $X$ and codomain $Z$) by $(g \circ f)(x) = g(f(x))$ $\forall x \in X$.

$f(x) \in Y$ $\forall x \in X$, so $g(f(x))$ is defined $\forall x \in X$.

$g \circ f$ is called the composition of $g$ and $f$

Examples of composition

① If $f_2 : (0,\infty) \longrightarrow \mathbb{R}$ and $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ as above,
then $f_1 \circ f_2 : (0,\infty) \longrightarrow \mathbb{R}$ is defined by $f_1 \circ f_2(x) = f_1\left(\frac{1}{x}\right) = \frac{1}{x^2}$

② $f_1 \circ f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $f_1 \circ f_1(x) = f_1(x^2) = x^4$.

③ $g \circ f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $g \circ f_1(x) = g(x^2) = 1 \ \forall x \in \mathbb{R}$

④ If $h : (0,\infty) \longrightarrow (0,\infty)$ is defined by $h(x) = \frac{1}{x} \ \forall x \in (0,\infty)$
then $h \circ h : (0,\infty) \longrightarrow (0,\infty)$ is defined by

$$h \circ h(x) = h\left(\frac{1}{x}\right) = \frac{1}{1/x} = x \ \forall x \in (0,\infty)$$

Defn The identity function $id_X$ on $X$ is the function
$id_X : X \longrightarrow X$ defined by $id_X(x) = x \ \forall x \in X$.

The image of a map/function

For a function $f : X \longrightarrow Y$, the image of $f$ is
the set $\{f(x) : x \in X\}$, called $Im(f)$.
Since $f(x) \in Y \ \forall x \in X$, we have $Im(f) \subset Y$.

This is related to the natural codomain used in MATH101
(The ~~natural codomai~~ image of $f$ is the natural codomain, if the domain is the "natural domain")

## Examples

(1) If $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ is given by $f_1(x) = x^2$ then

$\mathrm{Im}(f_1) = [0, \infty)$

(2) If $f_2 : \mathbb{R} \longrightarrow \mathbb{R}$ is given by $f_2(x) = x+1$

then the image of $f_2$, $\mathrm{Im}(f_2)$, is $\mathbb{R}$

because $x+1 = y \iff x = y-1$

(3) If $f_3 : [0, \infty) \longrightarrow \mathbb{R}$ is given by $f_3(x) = x+1$

then $\mathrm{Im}(f_3) = [1, \infty)$

(4) If $f : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $f(x) = x^3$ then $\mathrm{Im}(f) = \mathbb{R}$

(5) If $f : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $f(x) = x^2+1$

then $\mathrm{Im}(f) = [1, \infty)$.

$\mathrm{Im}(f) \subset [1, \infty)$ is clear because $x^2+1 \geq 1 \ \forall x \in \mathbb{R}$

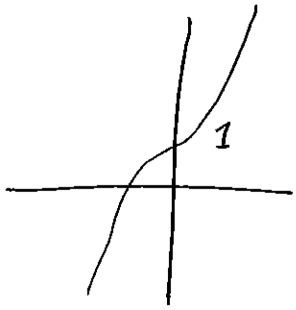
To see this: $x^2+1 = y \iff x^2 = y-1 \iff x = \sqrt{y-1}$ - defined finally $\geq 1$

So $\mathrm{Im}(f) = [1, \infty)$

(6) If $f : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $f(x) = x^3+x+1$ then

what is the image of $f$? It is $\mathbb{R}$, but that is

harder to prove.




Intuitively, just look at the graph.

All values are taken because arbitrarily large positive & negative values are taken

7. If $f: X \longrightarrow Y$ and $g: Y \longrightarrow Z$ are functions, show that $\mathrm{Im}(g \circ f) \subset \mathrm{Im}(g)$

If $z \in Z$ and $z \in \mathrm{Im}(g \circ f)$ then $z = g \circ f(x)$ for some $x \in X$

So $z = g(f(x))$ for some $x \in X$

So $z = g(y)$ for $y = f(x) \in Y$

So $z \in \mathrm{Im}(g)$

So $\mathrm{Im}(g \circ f) \subset \mathrm{Im}(g)$

## Surjective

Def$^n$ $f: X \longrightarrow Y$ is surjective or onto if $\mathrm{Im}(f) = Y$

that is, $\forall y \in Y \; \exists x \in X, \; f(x) = y$

Examples ① $f_1: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_1(x) = x^2$ is not surjective because $-1 \notin \mathrm{Im}(f_1)$ and $-1$ is in the codomain

② $f_2: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_2(x) = x+1$ is surjective because $\mathrm{Im}(f_2) = \mathbb{R}$. If $y \in \mathbb{R}$ then $f_2(y-1) = y$

③ $f_3: \mathbb{R} \longrightarrow \mathbb{R}$ given by $f_3(x) = x^3$ is surjective because $\mathrm{Im}(f_3) = \mathbb{R}$

④ So is $f_4: \mathbb{R} \rightarrow \mathbb{R}$ given by $f_4(x) = x^3 + x + 1$ (because $\mathrm{Im}(f_4) = \mathbb{R}$

⑤ Is $f: \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = x^2 + x + 1$ surjective?

No. because $f(x) = (x + 1/2)^2 + 3/4 \geq 3/4 \;\; \forall x \in \mathbb{R}$ So $\mathrm{Im}(f) \subset [3/4, \infty)$

In fact $\mathrm{Im}(f) = [3/4, \infty)$

(6) Is $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = e^x$ surjective ?
No, because $\mathrm{Im}(f) = (0, \infty)$ $\quad (f(\ln y) = y \quad \forall y > 0)$

(7) However $g: \mathbb{R} \to (0, \infty)$ given by $g(x) = e^x$ is surjective.

Injective

Defn $f: X \to Y$ is injective or one-to-one if
$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \forall x_1, x_2 \in X$. Equivalently:
$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \quad \forall x_1, x_2 \in X$

Examples (1) $f_1: \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x^2$ is not injective, because $f_1(1) = f_1(-1)$.

(2) $f_2: \mathbb{R} \to \mathbb{R}$ is injective because $f_2(x_1) = f_2(x_2)$
$\Leftrightarrow x_1 + 1 = x_2 + 1 \Leftrightarrow x_1 = x_2$

(3) $f: \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n^2$ is injective
because for $n, m \in \mathbb{N}$, $n^2 = m^2 \Leftrightarrow n = m$.
Is $f$ surjective ? (No, because $2 \notin \mathrm{Im}(f)$ )

(4) $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + x + 1$ is injective

$x^3 + x + 1 = y^3 + y + 1 \Leftrightarrow x^3 - y^3 + x - y = 0$

$\Leftrightarrow (x-y)(x^2 + xy + y^2 + 1) = 0$

$\Leftrightarrow (x-y)\left(\left(x + \tfrac{1}{2}y\right)^2 + \tfrac{3}{4}y^2 + 1\right) = 0$

$\Leftrightarrow x = y.$

A more straightforward way to show injectivity in this case is to show that $f$ is strictly increasing

Let $X, Y \subset \mathbb{R}$

<u>Def$^n$</u> A function $f: X \to Y$ is ~~stand~~ <u>increasing</u> if

$x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2) \quad \forall x_1, x_2 \in X$

$f$ is <u>strictly increasing</u> if $x_1 < x_2 \Rightarrow f(x_1) < f(x_2), \ \forall x_1, x_2 \in X$

$f$ is <u>decreasing</u> if $x_1 \leq x_2 \Rightarrow f(x_1) \geq f(x_2) \quad \forall x_1, x_2 \in X$

$f$ is <u>strictly decreasing</u> if $x_1 < x_2 \Rightarrow f(x_1) > f(x_2) \quad \forall x_1, x_2 \in X$

<u>Lemma</u> If $f: X \to Y$ is strictly increasing (or strictly decreasing) then $f$ is injective

<u>Proof</u> Suppose $x_1 \neq x_2$, $x_1, x_2 \in X$. We can assume $x_1 < x_2$

Then $f(x_1) < f(x_2)$ if $f$ is strictly increasing and $f(x_1) > f(x_2)$ if $f$ is strictly decreasing. In both cases $f(x_1) \neq f(x_2)$.

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

So $f$ is injective $\square$.

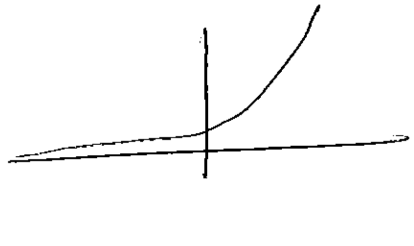
Applying this to the previous example, $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + x + 1$ is strictly increasing because

$x_1 < x_2 \Rightarrow x_1^3 < x_2^3 \wedge x_1 < x_2 \Rightarrow x_1^3 + x_1 + 1 < x_2^3 + x_2 + 1$

<u>Other examples.</u>

① $f(x) = e^x$, ~~is stri~~ $f: \mathbb{R} \to \mathbb{R}$, is strictly increasing

So injective



(2) $f:(0,\infty)\longrightarrow(0,\infty)$ given by $f(x)=\frac{1}{x}$ is strictly decreasing because $0<x<y \Rightarrow 0<1/y<1/x$

So $f$ is injective.

(3) $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=\sin x$ is not injective

$f(0)=f(\pi)$ – So not strictly increasing either. (and not increasing)

(4) $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=x+\sin x$ is strictly increasing; so must be injective.

Use calculus to show strictly increasing.

$f'(x) = 1+\cos x \geq 0$ with only isolated zeros at $(2n+1)\pi,\ n\in\mathbb{Z}$ – which makes $f$ strictly increasing.

In fact this map is also surjective, but in order to show that we need the Intermediate Value Theorem

## Bijections

Definition A function (map) ~~which~~ is bijective, called a bijection if it is both injective and surjective.

Examples (some of which we had before)

(1) $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=x+1$ is both surjective and injective, hence a bijection

(2) $f:\mathbb{R}\longrightarrow [0,\infty)$ given by $f(x)=x^2$ is not injective, hence not bijective (but it is surjective).

(3) However $g:[0,\infty)\longrightarrow[0,\infty)$ given by $g(x)=x^2$ is both injective and surjective, hence is a bijection.

4 $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is injective and surjective, hence a bijection. (Actually, ~~the~~ one way to show injective is to use $f$ strictly increasing, and one way to show surjective is to use $\lim_{x \to +\infty} f(x) = +\infty$, $\lim_{x \to -\infty} f(x) = -\infty$ and Intermediate Value Theorem.)

5 $f: \mathbb{N} \to \mathbb{N}$ defined by $f(n) = 2n$ is injective but not surjective, hence not a bijection.

6 $f: \mathbb{N} \to \mathbb{Z}$ defined by $f(n) = n$ is injective but not surjective, so not a bijection.

7 $f: \mathbb{N} \to \mathbb{Z}$ defined by

$$f(2n) = n \qquad \forall n \in \mathbb{N}$$
$$f(2n+1) = -n-1 \qquad \forall n \in \mathbb{N}$$

is ~~a~~ well-defined and is a bijection.

The even natural numbers map to all the natural numbers
The odd natural numbers map to all the strictly negative integers.

Let $f: X \longrightarrow Y$ be a function.

Def$^n$ The inverse function of $f$, $f^{-1}: Y \longrightarrow X$ (if it exists) is a function such that

$$f^{-1}(f(x)) = x \quad \forall x \in X$$
$$f(f^{-1}(y)) = y \quad \forall y \in Y$$

That is, $f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$

If an inverse function of $f: X \longrightarrow Y$ exists then it is unique. This was an exercise in MATH101 (Sheet 2)

If $g$ and $h$ both satisfy these properties then

$$g(f(x)) = x \quad \forall x \in X$$
$$f(h(y)) = y \quad \forall y \in Y$$

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

$\cancel{g(f(h(y)))=}$

This proves uniqueness.

Theorem $f: X \longrightarrow Y$ has an inverse $f^{-1} \Longleftrightarrow f$ is a bijection

Proof Suppose $f^{-1}$ exists. $f(f^{-1}(y)) = y \quad \forall y \in Y$

So $\mathrm{Im}(f) = Y$ and $f$ is surjective.

$f(x_1) = f(x_2) \Longrightarrow f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \Longrightarrow x_1 = x_2 \quad \forall x_1, x_2 \in X$

So $f$ is injective. So $f$ is bijective.

Now suppose $f$ is bijective. Define $g: Y \to X$ by $g(y) = x \Leftrightarrow f(x) =$

This is well defined because $x$ exists, given $y$, and is unique.

$g(f(x)) = x \;\; \forall x \in X$ $f(g(y)) = y \;\; \forall y \in Y$ So $g$ is the inverse of $f$ $\square$

**Corollary** If $f: X \to Y$ is a bijection so is $f^{-1}: Y \to X$

**Proof** $(f^{-1})^{-1} = f$ because $f \circ f^{-1} = id_Y$ $f^{-1} \circ f = id_X$ $\square$

**Examples**

① $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x+1$ has inverse

$f^{-1}(y) = y-1$ $\forall y \in \mathbb{R}$ $x+1 = y \Leftrightarrow x = y-1$

(or $f^{-1}(x) = x-1$ $\forall x \in \mathbb{R}$)

② $f: [0,\infty) \to [0,\infty)$ given by $f(x) = x^2$ has inverse

$f^{-1}(y) = \sqrt{y}$ $\forall y \in [0,\infty)$

③ $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ has inverse $f^{-1}(y) = y^{1/3}$ $\forall y \in \mathbb{R}$

④ $f: (-\infty,-1) \cup (-1,\infty) \to (-\infty,1) \cup (1,\infty)$ given by

$f(x) = \frac{x}{x+1}$. Find inverse $f^{-1}$

$\frac{x}{x+1} = y \Leftrightarrow x = xy + y \Leftrightarrow x(1-y) = y \Leftrightarrow x = \frac{y}{1-y}$

Defined for $y \neq 1$, and $x \neq -1$ for any $y \neq 1$

$f^{-1}(y) = \frac{y}{1-y}$ $\forall y \neq 1$

# Conditional and constructional definitions of sets

A <u>conditional definition</u> of a set is one of the form

$B = \{x : P(x)\}$ where $P(x)$ is a statement involving $x$

the set of $x$ such that $P(x)$

or, $B = \{x \in A : P(x)\}$

the set of $x$ in $A$ such that $P(x)$

A <u>constructional definition</u> of a set is one of the form

$B = \{f(x) : x \in X\}$ where $f : X \longrightarrow Y$ is some function with domain $X$ and some codomain $Y$. (It doesn't matter what $Y$ is so long as it is a valid codomain for this function)

So, of course, $B = Im(f)$, and the definition of $B$ is as the image of the function $f : X \longrightarrow Y$.

## Examples

Conditional definition:

$\{x \in \mathbb{R} : x \geqslant 0\}$ This is, of course, the set $[0, \infty)$

$\{n \in \mathbb{N} : 2 | n\}$ This is the set of even natural numbers.

Constructional definitions can be given for both these sets. For example

$\{x^2 : x \in \mathbb{R}\}$ is a constructional definition of the set $[0, \infty)$ : describes $[0, \infty)$ as the image of the set $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = x^2$.

$\{2n : n \in \mathbb{N}\}$ is a constructional definition of the set of even natural numbers.

This describes the set of even natural numbers as the image of the function $g : \mathbb{N} \to \mathbb{N}$ given by $g(n) = 2n$.

Example The set $\{3n+1 : n \in \mathbb{Z}\}$ is described constructively.

How to describe it conditionally? One way is $\{m \in \mathbb{Z} : 3 \mid m-1\}$ because $3 \mid m-1 \iff m-1 = 3n$ for some $n \in \mathbb{Z} \iff m = 3n+1$ for some $n \in \mathbb{Z}$.

## Finite and Infinite sets

Defn A set $A$ is finite if either $A$ is empty, or there is a bijection $f : \{k \in \mathbb{Z}_+ : 1 \le k \le n\} \to A$, for some $n \in \mathbb{Z}_+$.

If $A$ is not finite, then $A$ is said to be infinite.

Theorem If $m, n \in \mathbb{Z}_+$ and $m < n$, then there is no surjection from $\{k \in \mathbb{Z}_+ : k \le m\}$ to $\{k \in \mathbb{Z}_+ : k \le n\}$ and there is no injective map from $\{k \in \mathbb{Z}_+ : k \le n\}$ to $\{k \in \mathbb{Z}_+ : k \le m\}$.

Consequently, there is a bijection from $\{k \in \mathbb{Z}_+ : k \le m\}$ to $\{k \in \mathbb{Z}_+ : k \le n\}$ $\iff m = n$.

Proof By induction on $m$

Base case $m = 1$. If $f : \{k \in \mathbb{Z}_+ : k \le 1\} = \{1\} \to \{k \in \mathbb{Z}_+ : k \le n\}$ is a map, then $\operatorname{Im}(f) = \{f(1)\} \neq \{k \in \mathbb{Z}_+ : k \le n\}$ if $n > 1$

If $g : \{k \in \mathbb{Z}_+ : k \le n\} \to \{1\}$ is a map, then $g(n_1) = g(n_2)$ $\forall\, 1 \le n_1, n_2 \le n$.

So $g$ is not injective if $n > 1$.

Inductive step  Suppose the theorem is true for $m$, and for any $n > m$. Now consider $m+1$, and $n > m+1$

Suppose there is a surjection $f : \{k \in \mathbb{Z}_+ : k \leq m+1\} \rightarrow \{k \in \mathbb{Z}_+ : k \leq n\}$

Define $g : \{k \in \mathbb{Z}_+ : k \leq m\} \longrightarrow \{k \in \mathbb{Z}_+ : k \leq n-1\}$ key

$$
\begin{aligned}
g(k) &= f(k) \text{ if } k \leq m \text{ and } f(k) \leq n-1 \\
&= f(m+1) \text{ if } f(k) = n \text{ and } f(m+1) \leq n-1 \\
&= \cancel{f}\ 1 \quad \text{if } f(k) = n = f(m+1)
\end{aligned}
$$

Then $g$ is surjective, which is a contradiction, because $m < n-1$
So there is no such surjection $f$.
Now suppose there is an injective map ~~$f : \{k \in \mathbb{Z}_+ : k \leq n+1\} \rightarrow \{k \in \mathbb{Z}_+ : k \leq m\}$~~

$$f : \{k \in \mathbb{Z}_+ : k \leq n\} \longrightarrow \{k \in \mathbb{Z}_+ : k \leq m+1\}$$

Define $g : \{k \in \mathbb{Z}_+ : k \leq n-1\} \longrightarrow \{k \in \mathbb{Z}_+ : k \leq m\}$ key

$$
\begin{aligned}
g(k) &= f(k) \text{ if } f(k) \leq m \\
g(k) &= f(n) \text{ if } f(k) = m+1
\end{aligned}
$$

Then $g(k) \leq m$ $\forall k \leq n-1$ because $f$ is injective, so $f(k) \neq f(n)$ if $k < n$.

$f$ injective $\Rightarrow$ $g$ injective, ~~that~~ contradicting what is true for $m$.

So there is no such injective $f$.

~~So~~ So theorem true for $n$ $\Rightarrow$ Theorem true for $n+1$.

So by induction the theorem is true for all $n$.

<u>Definition</u> A ~~finite~~ set $A$ <u>has $n$ elements</u> if there is a bijection $f : \{k \in \mathbb{Z}_+ : k \le n\} \to A$.

We then write $|A| = n$.

<u>Def$^n$</u> A set $A$ <u>has 0 elements</u> if $A = \emptyset$.

By the theorem just proved, a set cannot have $n$ elements, and also have $m$ elements, if $n \neq m$. Otherwise there would be a bijection from $\{k \in \mathbb{Z}_+ : k \le m\}$ to $\{k \in \mathbb{Z}_+ : k \le n\}$

<u>Def$^n$</u> We also say that $A$ <u>has cardinality $n$</u> if $A$ has $n$ elements.

<u>Examples</u> $\{1, 2, 4\}$ has 3 elements. $f : \{1, 2, 3\} \to \{1, 2, 4\}$ defined by $f(1) = 1$, $f(2) = 2$, $f(3) = 4$ is a bijection.

$\{k \in \mathbb{N} : k < n\}$ has $n$ elements because $f : \{k \in \mathbb{Z}_+ : k \le n\} \to \{k \in \mathbb{N} : k < n\}$ is a bijection with $f(k) = k - 1$.

## <u>Working with sets.</u>

Recall that
$$A \cup B = \{x : x \in A \vee x \in B\}$$
$$A \cap B = \{x : x \in A \wedge x \in B\}$$
$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

## Standard Identities

1. $A \cup (B \cup C) = (A \cup B) \cup C$ ) Associativity
2. $A \cap (B \cap C) = (A \cap B) \cap C$
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ) Distributivity
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$
6. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
7. $A = (A \setminus B) \cup (A \cap B)$ Every elt of $A$ is either in $B$ or not in $B$
8. $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$

Defn We write $|A| = n$ if $A$ has elements

Defn We say $A$ and $B$ are disjoint if $A \cap B = \emptyset$.

Counting and Set Theory

Theorem If $A$ and $B$ are disjoint finite sets then

$$|A \cup B| = |A| + |B|$$

Proof Let $|A| = m$ and $|B| = n$.
We want to show $|A+B| = m+n$.
There are bijections $f: \{k \in \mathbb{Z}_+ : k \le m\} \to A$ and $g: \{k \in \mathbb{Z}_+ : k \le n\} \to B$

Define $h: \{k \in \mathbb{Z}_+ : k \le m+n\} \to A \cup B$ by

$$h(k) = f(k) \text{ if } k \le m$$
$$= g(k-m) \text{ if } k > m$$

Then $h$ is well-defined, injective because $A$ and $B$ are disjoint and $f$ & $g$ injective and surjective because $f$ and $g$ are surjective. So $h$ is a bijection

By induction on this we can prove, for any $n \geq 2$ if $A_j$ are finite,

$$\left|\bigcup_{j=1}^{n} A_j\right| = \sum_{j=1}^{n} |A_j| \quad \text{if } A_j \cap A_k = \emptyset \text{ for all } j \neq k$$

In particular if $A_1 \cap A_2 = A_2 \cap A_3 = A_1 \cap A_3 = \emptyset$ then

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3|$$

<u>Corollary</u> For any 2 finite sets $A$ and $B$,

$$|A| = |A \setminus B| + |A \cap B|$$
$$|B| = |B \setminus A| + |A \cap B|$$
$$|A \cup B| = |A| + |B| - |A \cap B|,$$ the <u>Inclusion-Exclusion Principle for 2 sets</u>

<u>Proof</u> $A \setminus B$ and $A \cap B$ are disjoint and
$A = (A \setminus B) \cup (A \cap B)$. ①

So $|A| = |A \setminus B| + |A \cap B|$

Similarly, $|B| = |B \setminus A| + |A \cap B|$. ②

$A \setminus B$, $B \setminus A$ and $A \cap B$ are disjoint and

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

So $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B|$ ③

③ − ② − ① gives

$$|A \cup B| - |A| - |B| = -|A \cap B|$$ $\square$

or $|A \cup B| = |A| + |B| - |A \cap B|$.

<u>Example</u> If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$

then $A \cap B = \{2, 3\}$ and $A \cup B = \{1, 2, 3, 4\}$

$|A \cup B| = 4$ $\quad |A| = |B| = 3$ $\quad |A \cap B| = 2$

$3 + 3 - 2 = \cancel{4}\ 4$ ✓

## Inclusion– ~~and~~ Exclusion principle for 3 sets

$$|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |A\cap C| - |C\cap B| + |A\cap B\cap C|$$

<u>Proof</u> Use the Inclusion-exclusion principle for 2 sets twice.

$$|A\cup B\cup C| = |A| + |B\cup C| - |A\cap(B\cup C)|$$

$$= |A| + |B| + |C| - |B\cap C| - |(A\cap B)\cup(A\cap C)|$$

$$= |A| + |B| + |C| - |B\cap C| - \Big(|A\cap B| + |A\cap C| - \underbrace{|A\cap B\cap C|}_{\therefore\ (A\cap B)\cap(A\cap C)}\Big)$$

$$= |A| + |B| + |C| - |B\cap C| - |A\cap B| - |A\cap \quad + |A\cap B\cap C|$$

## Inclusion exclusion in general

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1<i_2<\dots<i_k} \left|\bigcap_{j=1}^{k} A_{i_j}\right|$$

See Eccles Problems III. 4.

Quick example of inclusion-exclusion principle for 3 sets

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

$A\cup B\cup C = \{1,2,3,4,5\}$   $(A\cap B| = \{2,3\}$   $A\cap B\cap C = \{3\}$

$B\cap C = \{3,4\}$   $A\cap C = \{3\}$

$|A\cup B\cup C| = 5$   $|A| + |B| + |C| - |A\cap B| - |B\cap C| - |C\cap A| + |A\cap B\cap C|$

$= 3 + 3 + 3 - 2 - 2 - 1 + 1 = 5$ ✓

~~4~~ (S2)

Example

(1) There are 500 students who are doing either MATH 111 or ECON 121 or both.

160 are doing MATH111
400 are doing ECON121

How many are doing both?

$|M| = 160$ $\quad |E| = 400$

$|M \cup E| = 500$

$|M \cup E| = 500 = |M| + |E| - |M \cap E| = 160 + 400 - |M \cap E|$

$|M \cap E| = 160 + 400 - 500 = 60.$

(2) 700 students are doing at least one of MATH111 or ECON121 or PSYC101

160 are doing MATH 111 — M
400 — ECON121 — E
350 — PSYC — P

5 are doing all 3.

How many are doing exactly 2?

$|M \cup E \cup P| = 700 = |M| + |E| + |P| - |M \cap E| - |E \cap P| - |M \cap P| + |M \cap E \cap P|$

$= 910 - |M \cap E| - |E \cap P| - |M \cap P| + 5$

$|M \cap E| + |E \cap P| + |M \cap P| = 215$

$|M \cap E \setminus P| + |E \cap P \setminus M| + |M \cap P \setminus E|.$

Exactly 2 $= |M \cap E \setminus P| + |E \cap P \setminus M| + |M \cap P \setminus E|$

$= (|M \cap E| - |M \cap E \cap P|) + (|E \cap P| - |M \cap E \cap P|) + (|M \cap P| - |M \cap P \cap E|)$

$= 215 - 3 \times 5 = 200.$

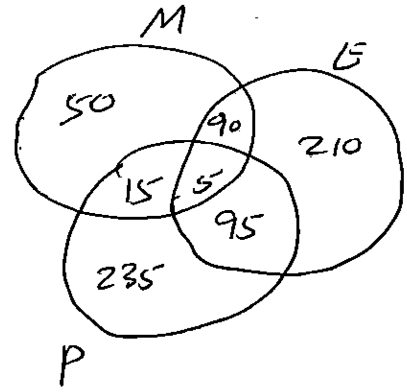
If ~~100~~ 20 are doing PSYC101 and MATH111 and ~~20~~ 100 are doing both ECON121 and PSYC101, how many are doing both ECON121 and MATH111?

$|M \cap P| = \cancel{100}\ 20 \qquad |E \cap P| = \cancel{20}\ 100$

$700 = 910 - |M \cap E| - |M \cap P| - |E \cap P| + 5$

$= 915 - |M \cap E| - 120$

$|M \cap E| = 915 - 820 = 95.$



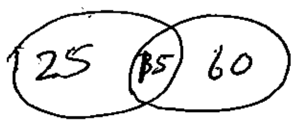

<u>Another example</u>

a) 100 farms in an area have either crops or animals or both. If 75 farms have crops and 40 have animals, how many have both?

$|A \cup C| = 100 \qquad |A| = 40 \qquad |C| = 75$

$|A \cap C| = -|A \cup C| + |A| + |C| = -100 + 115 = 15$

15 have both.

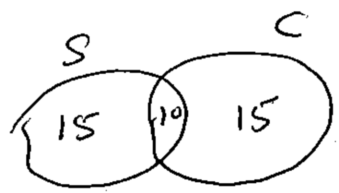



b) Of the ~~70~~ 40 farms that have animals, the animals are all sheep or cattle. 25 have sheep and 10 have both sheep and cattle. How many have cattle?

$|S \cup C| = \cancel{70}\ 40 \qquad |S| = 25 \qquad |S \cap C| = 10$

$\cancel{70}\ 40 = |S \cup C| = |S| + |C| - |S \cap C| = 25 + |C| - 10$

$|C| = \cancel{70}\ 40 - 15 = \cancel{55}\ 25$



c) Now let's consider the 75 farms that have crops

The possible crops are wheat, beet or potatoes

44 farms have wheat. 38 have beet. 27 have potatoes

4 farms grow all 3. 14 grow wheat and beet.

13 grow wheat and potatoes.

How many grow beet and potatoes?

$|W \cup P \cup B| = 75 \quad |W| = 44 \quad |B| = 38 \quad |P| = 27$

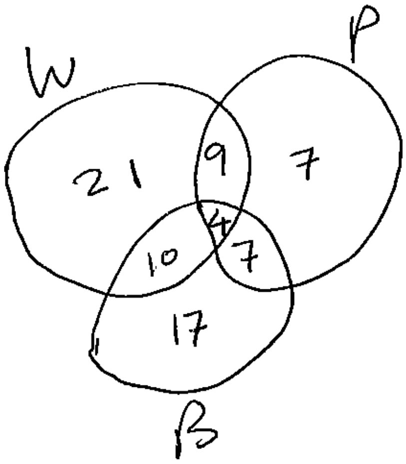
$|W \cap B| = 14 \quad |W \cap P| = 13 \quad |W \cap P \cap B| = 4$

$$|W \cup P \cup B| = |W| + |B| + |P| - |W \cap B| - |W \cap P| - |B \cap P| + |W \cap P \cap B|$$

$$75 = 44 + 38 + 27 - 14 - 13 - |B \cap P| + 4$$

$$75 = 109 - 27 + 4 - |B \cap P|$$

$$|B \cap P| = 86 - 75 = 11$$



56

## Product sets

Most of this will not be lectured.

**Defn** If $X$ and $Y$ are non-empty sets, then the *product of $X$ and $Y$*, denoted by $X \times Y$, is the set $\{(x,y) : x \in X, y \in Y\}$

$X \times X$ is often denoted by $X^2$

e.g. $\mathbb{R}^2 = \{(x,y) : x, y \in \mathbb{R}\}$

$X^2$ can also be thought of as the set of functions from $\{1,2\}$ to $X$ because there is a bijection

$$F : \{(x_1, x_2) : x_1, x_2 \in X\} \longrightarrow \{f : f \text{ is a function from } \{1,2\} \text{ to } X\}$$

defined by

$$F(x_1, x_2) = f \text{ where } f(1) = x_1 \quad f(2) = x_2$$
$$f : \{1,2\} \longrightarrow X$$

Similarly if $X_i \neq \phi$ for $1 \leq i \leq n$ then

$$X_1 \times \cdots \times X_n = \{(x_1, x_2 \ldots x_n) : x_i \in X_i, \ 1 \leq i \leq n\}$$

$$X^n = \{(x_1, x_2 \ldots x_n) : x_i \in X, \ 1 \leq i \leq n\}$$

There is a natural bijection ~~fro~~

$$F : X^n \longrightarrow \{f : f \text{ is a function from } \{k \in \mathbb{Z}_+ : k \leq n\} \text{ to } X\}$$

defined by $F(x_1, \ldots x_n) = f$ where $f(i) = x_i$
$$f : \{k \in \mathbb{Z}_+ : k \leq n\} \to X.$$

$X^n$ is actually a shorthand for $X^{\{k \in \mathbb{Z}_+ : k \leq n\}}$

<u>Theorem</u> If $X$ and $Y$ are finite sets then $X \times Y$ is finite and $|X \times Y| = |X| . |Y|$

Proof Since there are $n, m \in \mathbb{Z}_+$ ~~such that~~ and bijections from $\{k \in \mathbb{Z}_+ : k \leq n\}$ to $X$ and from $\{k \in \mathbb{Z}_+ : k \leq m\}$ to $Y$, it suffices to find a bijection from $\{k \in \mathbb{Z}_+ : k \leq mn\}$ to $\{k \in \mathbb{Z}_+ : k \leq n\} \times \{k \in \mathbb{Z}_+ : k \leq m\}$

Write $k = n k_2 + k_1$ with $0 \leq k_2 < m$ and $1 \leq k_1 \leq n$

and define $F(k) = (k_1, k_2 + 1)$

<u>Corollary</u> If $X_1 \ldots X_n$ are finite then $|X_1 \times \cdots \times X_n|$ has $|X_1| \times \cdots \times |X_n|$ elements.

If $X$ is finite then $X^n$ has $|X|^n$ elements.

<u>Powers Sets</u>

If $X$ is any set then $P(X)$ or $2^X$ denotes the set $\{Y : Y \subseteq X\}$. This is called the <u>power set of $X$</u>.

<u>Examples</u> $P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

$P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$

Why the notation $2^X$?

Because $|2^X| = \cancel{\$}\, 2^{|X|}$ and there is a natural bijection from $P(X)$ to the set of functions from $X$ to $\{1,2\}$