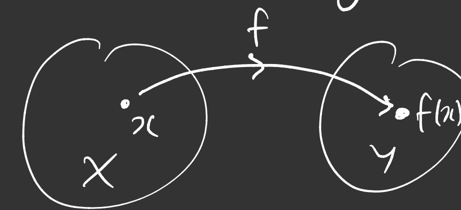
Lecture 5

Functions

Definition Let X and Y be sets. A **function**, or **map**, $f: X \to Y$ is an assignment of a value $f(x) \in Y$ to every $x \in X$.

X is called the **domain**, and Y is the **codomain**.



Examples $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$

$f: \mathbb{R} \to \mathbb{Z}$ defined by the rule that $f(x)$ is the least integer that is larger than or equal to x. This is the **ceiling** function $\lceil x \rceil$.

Remark The definition of the function must assign a unique value of $f(x)$ to every $x \in X$.

eg. $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = 1/x$ would be an **ill-defined** function.
(it does not provide a recipe for $x = 0$).

$f: \mathbb{Q} \to \mathbb{Z}$ given by $f\left(\frac{m}{n}\right) = n$ is **not well-defined** since it does not assign a unique value for every $q \in \mathbb{Q}$.

Definitions Given a function $f: X \to Y$, the *image*, or *range*, is

$$f(X) = \{ f(x) : x \in X \} \subseteq Y$$

If $A \subseteq X$, the *image of A* under f is $f(A) = \{ f(x) : x \in A \} \subseteq Y$

If $B \subseteq Y$, the *pre-image* of B under f is $f^{-1}(B) = \{ x \in X : f(x) \in B \} \subseteq X$

Examples $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, has $f(\mathbb{R}) = [0, \infty)$, $f([0,1]) = [0,1]$ and $f^{-1}([0,1]) = [-1,1]$.

The ceiling function has $f(\mathbb{R}) = \mathbb{Z}$, and $f^{-1}(\{n\}) = (n-1, n]$

Definition Given a function $f: X \to Y$, and a subset $A \subseteq X$, the *restriction* of f to A is $f|_A : A \to Y$ is defined by $f|_A(x) = f(x)$. for all $x \in A$.

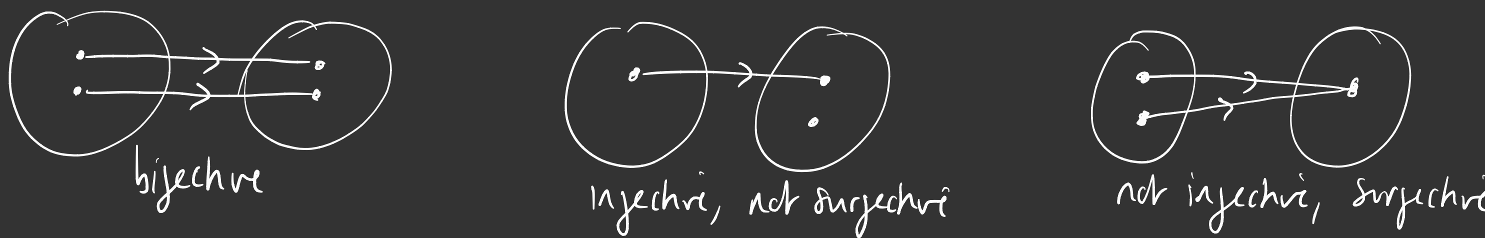
Definition Given a set X, the *identity map* $id_X : X \to X$ is defined by $id_X(x) = x$ for all $x \in X$.

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

(i) f is injective, or one-one (1-1), if whenever $f(x_1) = f(x_2)$ then $x_1 = x_2$

(ii) f is surjective, or onto, if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

(iii) f is bijective, and is called a bijection, if it is injective and surjective.



Examples $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is neither injective nor surjective.

$f: [0,\infty) \to [0,\infty)$ " is injective and surjective.

$f: \mathbb{R} \to [0,\infty)$ " is not injective, but it is surjective.

The ceiling function is surjective, but not injective.

Lecture 5b

Definition (cardinality of a finite set). A non-empty set S is finite and has cardinality $n \in \mathbb{N}$ if there exists a bijection from $\{1, 2, \dots, n\}$ to S.

Note that if X and Y are finite sets, and $f: X \to Y$ is injective, then $|Y| \geq |X|$.
This is the pigeonhole principle. If f is surjective, then $|X| \geq |Y|$.
If f is bijective, then $|X| = |Y|$.

Definition Let $f: X \to Y$ and $g: Y \to Z$ be functions. The composition $g \circ f: X \to Z$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

If $X = Y = Z$, we can also define $f \circ g$, but $f \circ g \neq g \circ f$.

eg. $X = Y = Z = \mathbb{R}$, and $f(x) = x^2$, $g(x) = e^x$. Then $(f \circ g)(x) = e^{2x}$, $(g \circ f)(x) = e^{x^2}$

Definition A function $f: X \to Y$ is *invertible* if there exists $g: Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. g is the *inverse* of f, and we write $g = f^{-1}$.

Proposition If $f: X \to Y$ is invertible then the inverse is unique.

proof: Suppose g_1 and g_2 are both inverses. ie $g_i \circ f = \mathrm{id}_X$ and $f \circ g_i = \mathrm{id}_Y$ for $i = 1, 2$.

$$g_1 = g_1 \circ \mathrm{id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2$$

[composition of functions is associative] $\square$

<u>Theorem</u> A function $f: X \to Y$ is invertible if and only if it is bijective.

<u>proof</u>: Suppose f is invertible. So there exists g such that $g \circ f = id_X$ and $f \circ g = id_Y$.

We need to show (NTP) that f is injective and f is surjective.

To show f is injective, suppose $f(x_1) = f(x_2)$, then applying g gives $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. So f is injective. To show f is surjective, note that for any $y \in Y$, there exists $x = g(y) \in X$ such that $f(x) = f(g(y)) = y$. So f is surjective. Hence f is bijective.

Conversely, suppose f is bijective. We need to define an inverse $g: Y \to X$. Note that for any $y \in Y$, $\exists\, x \in X$ s.t. $f(x) = y$ (since f is surjective) and moreover that x is unique (since f is injective). This provides a recipe to construct a map $x = g(y)$ that is well-defined and has the properties $f(g(y)) = y$ & $g(f(x)) = x$. So f is invertible.

$\square$

Lecture 6

Handling logical notation and quantifiers

Remarks about 'if P then Q' or '$P \Rightarrow Q$'

- The following mean the same:

  if P then Q, $P \Rightarrow Q$, P only if Q, whenever P holds then Q holds,

  P is sufficient for Q, Q is necessary for P,

  if Q is not true then P is not true ← contrapositive
- To prove such a statement either suppose P is true and show Q is true, or suppose Q is not true and show that P is not true.
- Note that the contrapositive is not the same as the converse (if Q then P, $Q \Rightarrow P$), which is a different statement.
- To disprove such a statement, we need to find some circumstance under which P is true and Q is not true.
- No causality is implied by saying 'if P then Q'
- If P is never true, the statement 'if P then Q' is vacuously true.

- Don't mix and match 'if... then...' and $\Rightarrow$, eg. If $x=-1 \Rightarrow x^2=1$

eg. $x^2+2x+1=0$ I suggest not to use $\Rightarrow$ to connect every line of

$(x+1)^2=0$ working, but reserve it for use in more concise statements.

$x=-1$

<u>Remarks</u> about 'P if and only if Q', '$P \Leftrightarrow Q$'

- Usually best to treat such statements separately as $P \Rightarrow Q$ and $Q \Rightarrow P$.
- Sometimes it may be helpful to read these statements as 'P is equivalent to Q'.

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

<u>Remark</u> about 'or'

- $P \vee Q$ means P is true or Q is true or both are true.
- If we mean exclusive or, write 'P or Q, but not both', or $(P \wedge \neg Q) \vee (\neg P \wedge Q)$

Lecture 6b

Remarks about quantifiers

- These are most useful for providing concise statements of definitions. eg. if $f: X \to Y$,

  f is injective if $\quad \forall x_1, x_2 \in X,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

  f is surjective if $\quad \forall y \in Y,\ \exists x \in X$ s.t. $f(x) = y$.

- We should specify the set to which the quantifier relates,

  eg. don't write $\forall x,\ x^2 \geq 0$.

  However, in Analysis, we might write things like '$\forall \varepsilon > 0, \ldots$' in which it is understood that ε is a real number.

- To prove a statement of the form '$\forall x \in X, \ldots$', we should start the proof with 'Let $x \in X$.' and treat x as fixed for the rest of the proof.

  [The proof could also start 'Given $x \in X, \ldots$']

Remark about the order of quantifiers.

Suppose S is the set of students at Oxford, and C is the set of colleges.

Consider the statement

$$(*) \quad \forall s \in S,\ \exists c \in C \text{ s.t. } s \in c$$

$$\exists c \in C \text{ s.t. } \forall s \in S,\ s \in c$$

We should read from left to right, and any element introduced by a quantifier can depend on previously introduced elements, but not ones that are yet to be introduced.

Remark about negation of quantifiers

If P is the statement '$\forall x \in X,\ Q(x)$', not P is '$\exists x \in X$ s.t. $Q(x)$ is not true'

If P is the statement '$\exists x \in X$ s.t. $Q(x)$', not P is '$\forall x \in X$, $Q(x)$ is not true'

To negate a statement involving quantifiers, change $\forall$ to $\exists$, and vice versa, and negate the statement to which they relate.

eg. the negation of $(*)$ is $\exists s \in S$ s.t. $\forall c \in C,\ s \notin c$

Lecture 7

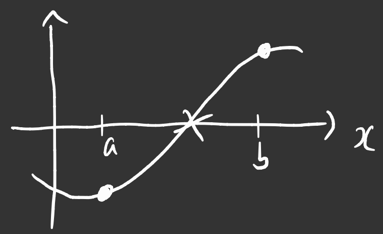
Constructing mathematical statements and proofs

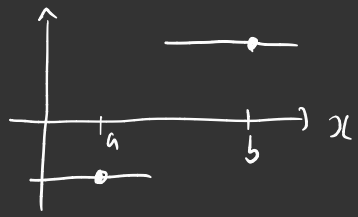
Formulation of mathematical statements

Most theorems are of the overall structure 'if P then Q'

P is called the <u>hypothesis</u>, Q is the <u>conclusion</u>.

<u>Intermediate value theorem</u>. Let $f: \mathbb{R} \to \mathbb{R}$ be a continuous function, and suppose $a, b \in \mathbb{R}$, with $a < b$, $f(a) < 0$, and $f(b) > 0$. Then there exists $c \in (a,b)$ with $f(c) = 0$.





eg. 'every prime number greater than 2 is odd'

'Let p be a prime number greater than 2. Then p is odd'

Theorem (AM-GM inequality). Let x, y be non-negative real numbers. Then $\sqrt{xy} \leq \frac{1}{2}(x+y)$

Direct proof Assume P is true, and use a sequence of logical steps to arrive at Q.

eg. Note that $(x-y)^2 \geq 0$. So $x^2 - 2xy + y^2 \geq 0$. Adding $4xy$ gives $(x+y)^2 \geq 4xy$. Square root (noting $x, y \geq 0$) to get $\frac{1}{2}(x+y) \geq \sqrt{xy}$. $\square$

Proof by contradiction Assume P is true, suppose Q is not true, and arrive at a contradiction.

eg. Suppose, for a contradiction, that $\sqrt{xy} > \frac{1}{2}(x+y)$. Then $4xy > (x+y)^2 = x^2 + 2xy + y^2$, so $0 > (x-y)^2$, which is a contradiction. ※. Hence $\sqrt{xy} \leq \frac{1}{2}(x+y)$. $\square$

Proof by induction Useful to prove statements indexed by $\mathbb{N}$.

eg. Let $x_1, x_2, \ldots, x_n$ be non-negative real numbers. Then $(x_1 x_2 \cdots x_n)^{1/n} \leq \frac{1}{n}(x_1 + x_2 + \cdots + x_n)$

<u>Least criminal</u> (combination of induction and contradiction). If proving statements $Q(n)$, we suppose a contradiction. There must be a least n for which $Q(n)$ is not true, so focus on ~~that~~ n, and look for a contradiction.

eg. to show $n+n^2$ is even for all $n \in \mathbb{N}$, suppose that is not true. Then there is a least n, call it k, such that $k+k^2$ is odd. Then $(k-1)+(k-1)^2 = k+k^2-2k$ is also odd, which contradicts the minimality of k.

<u>Counterexamples</u> (for refuting or disproving a statement).

Look for simple or extreme cases as counterexamples.

eg. <u>Claim</u> Let x, y be real numbers. Then $\sqrt{|xy|} \leq \frac{1}{2}(x+y)$.

<u>Refutation</u>: this is not true. A counterexample is $x=1, y=-1$.

Lecture 7b

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

(i) If f and g are injective, then $g \circ f$ is injective. Conversely, if $g \circ f$ is injective, then f is injective, but g need not be.

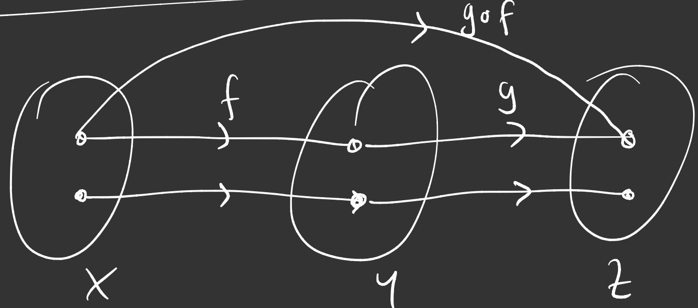
(ii) If f and g are surjective, then $g \circ f$ is surjective. Conversely, if $g \circ f$ is surjective, then g is surjective, but f need not be.

proof of (i). Suppose f and g are injective. Need to show $g \circ f$ is injective. Let $x_1, x_2 \in X$ have $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then $g(f(x_1)) = g(f(x_2))$, and since g is injective this means $f(x_1) = f(x_2)$. Then since f is injective, this means $x_1 = x_2$. So $g \circ f$ is injective.

Thoughts: f is injective $\iff$ $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.

Conversely, suppose $g \circ f$ is injective. Need to show f is injective. Suppose, for a contradiction, that f is not injective. Then there exist $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$. Then $(g \circ f)(x_1) = (g \circ f)(x_2)$, which contradicts $g \circ f$ being injective. So f is injective.

To see that g need not be injective, take $X = \{0\} = Z$ and $Y = \{0, 1\}$, and $f(0) = 0$ and $g(0) = 0, g(1) = 0$. $\square$



General advice on constructing proofs

- Be clear about hypotheses and conclusions.
- Unpack any definitions. Restate what you know, and what you need to show.
- If you can't progress directly, try 'seeking a contradiction'.
- If showing uniqueness, suppose there are two of the things, and show they are equal.
- Look for extreme / simple cases as counterexamples.
- Don't be afraid to experiment, but have in mind what you're aiming for.
- Draw diagrams to gain intuition.
- Re-read your final proof. Be critical, and check you're convinced.

Lecture 8

Problem solving examples

Example. (Images and preimages). Let $f\colon X \to Y$ be a mapping and let $A, B \subseteq X$ and $C, D \subseteq Y$. Are the following statements true or false?

(i) $f(A \cap B) = f(A) \cap f(B)$,

(ii) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

(i) False. A counterexample is $f: \mathbb{R} \to \mathbb{R}$ given by $f(x) = 0$ for all $x \in \mathbb{R}$. Then if $A = \{0\}$ and $B = \{1\}$, then $f(A \cap B) = \emptyset$ and $f(A) \cap f(B) = \{0\}$.

(ii) True. proof: Suppose $x \in f^{-1}(C \cap D)$. Then $f(x) \in C \cap D$, so $f(x) \in C$ and $f(x) \in D$. Then $x \in f^{-1}(C)$ and $x \in f^{-1}(D)$, and hence $x \in f^{-1}(C) \cap f^{-1}(D)$. So LHS $\subseteq$ RHS.

Conversely, if $x \in f^{-1}(C) \cap f^{-1}(D)$, then $x \in f^{-1}(C)$ and $x \in f^{-1}(D)$, so $f(x) \in C$ and $f(x) \in D$. Hence $f(x) \in C \cap D$, and therefore $x \in f^{-1}(C \cap D)$. So RHS $\subseteq$ LHS.

So LHS = RHS. $\square$

Alternative proof:

$$\begin{aligned} x \in f^{-1}(C \cap D) &\iff f(x) \in C \cap D \\ &\iff f(x) \in C \text{ and } f(x) \in D \\ &\iff x \in f^{-1}(C) \text{ and } x \in f^{-1}(D) \\ &\iff x \in f^{-1}(C) \cap f^{-1}(D) \end{aligned}$$ $\square$

Example. (Modular arithmetic). Let $n \geq 2$ be an integer and let $\mathbb{Z}_n$ be the set of equivalence classes $\{\overline{0}, \overline{1}, , \ldots, \overline{n-1}\}$ defined by congruence modulo n on $\mathbb{Z}$.

(i) Show that the operation $\otimes$ on $\mathbb{Z}_n$ defined by

$$\overline{x} \otimes \overline{y} = \overline{x \times y},$$

is well-defined, where $x \times y$ denotes standard muliplication on $\mathbb{Z}$.

(ii) If $\overline{x} \neq \overline{0}$, a multiplicative inverse $\overline{y}$ has the property that $\overline{x} \otimes \overline{y} = \overline{1}$. Is there a multiplicative inverse for every $\overline{x} \neq \overline{0}$? What if n is prime?

[*You may assume Bezout's lemma, which says that if integers a and b are coprime, there exist integers k and l such that $a \times k + b \times l = 1$.*]

Note that $x \sim y \Leftrightarrow y - x$ is a multiple of n.

(i) Need to show that if $\overline{x_1} = \overline{x_2}$ and $\overline{y_1} = \overline{y_2}$ then $\overline{x_1 y_1} = \overline{x_2 y_2}$ (we omit $\times$ for brevity)

Note that $x_2 - x_1 = kn$ and $y_2 - y_1 = ln$ for some integers k, l.

So $x_2 y_2 = (x_1 + kn)(y_1 + ln) = x_1 y_1 + \underbrace{kny_1 + lnx_1 + kln^2}_{(ky_1 + lx_1 + kln)n}$, so $\overline{x_2 y_2} = \overline{x_1 y_1}$

Hence $\otimes$ is well-defined.

(ii) For general n, there is not necessarily a multiplicative inverse for every $\bar{x} \neq \bar{0}$.

eg. for $n=4$, $\bar{2}$ does not have an inverse.

For n prime, the equivalence classes are $\bar{x}$ for $0 \leq x < n$. For $1 \leq x < n$, x and n are coprime, so the lemma tells us that there exist integers k and l such that $xk + nl = 1$. Then $\overline{xk} = \bar{1}$, ie. $\bar{x} \otimes \bar{k} = \bar{1}$. So $\bar{k}$ is the multiplicative inverse of $\bar{x}$. Hence all $\bar{x} \neq 0$ have a multiplicative inverse in the case when n is prime.

Lecture 8b

Example. (Limits). A continuous function $f\colon \mathbb{R} \to \mathbb{R}$ tends to zero as $x \to \infty$ if

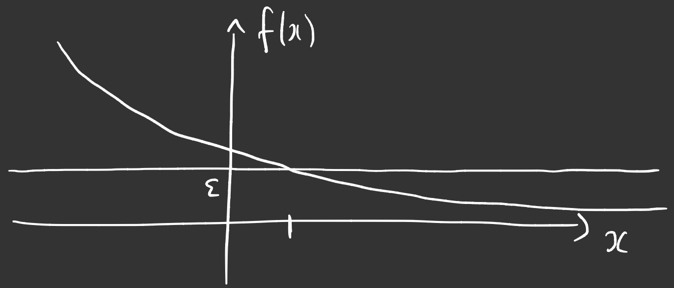
$$\forall \varepsilon > 0,\ \exists X \in \mathbb{R} \text{ s.t. } \forall x \in \mathbb{R},\ \text{if } x > X \text{ then } |f(x)| < \varepsilon.$$

Prove or disprove whether the following functions tend to zero as $x \to \infty$:

(i) $f(x) = e^{-x}$;

(ii) $f(x) = \cos x$.

(i)



$$e^{-X} = \varepsilon \iff X = -\ln \varepsilon$$

Let $\varepsilon > 0$ be given. Then let $X = -\ln \varepsilon$. Then $\forall x \in \mathbb{R}$, if $x > X$ then

$$|f(x)| = |e^{-x}| < |e^{-X}| = \varepsilon$$

Hence f tends to zero as $x \to \infty$.

Example. (Limits). A continuous function $f: \mathbb{R} \to \mathbb{R}$ tends to zero as $x \to \infty$ if

$$\forall \varepsilon > 0,\ \exists X \in \mathbb{R} \text{ s.t. } \forall x \in \mathbb{R},\ \text{if } x > X \text{ then } |f(x)| < \varepsilon.$$

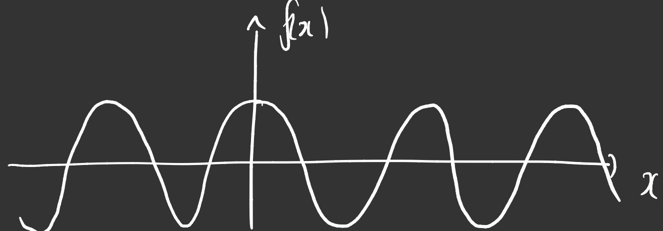
Prove or disprove whether the following functions tend to zero as $x \to \infty$:

(i) $f(x) = e^{-x}$;

(ii) $f(x) = \cos x$.

(ii) Note that the negation of the given definition is

$$\exists\, \varepsilon > 0 \text{ s.t. } \forall X \in \mathbb{R},\ \exists\, x \in \mathbb{R} \text{ s.t. } x > X \text{ and } |f(x)| \geq \varepsilon$$



Take $\varepsilon = \frac{1}{2}$, and let $X \in \mathbb{R}$ be given. Then there exists $x = 2\pi n$ (for some $n \in \mathbb{Z}$) such that $x > X$, and $|f(x)| = 1 \geq \varepsilon$.

Hence $f(x) = \cos x$ does not tend to zero as $x \to \infty$.