A <u>set</u> is a collection of elements.

$R = \{0, 1, 2\}$

$S = \{n^2, 2^n, n!\}$

$T = \{a, 42, R\}$

We write $0 \in R$ to say R <u>contains</u> 0 and $n^2 \notin R$ to say R does not contain n^2.
We denote the <u>size</u> of a set A by $|A|$.

<u>Useful sets</u>

$\mathbb{N} = \{1, 2, 3, \ldots\}$ (often contains 0)
(when $|S| \leq |\mathbb{N}|$, we say S is <u>countable</u> or <u>ennumerable</u>)

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

$\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$

$\mathbb{R}$ = the completion of $\mathbb{Q}$

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

$\emptyset = \{\}$

<u>Set operations</u>

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

$A \cap B = \{g \mid g \in A \text{ and } g \in B\}$

$\bar{A} = \{g \mid g \notin A\}$ (complements are relative to some universe)

$A \setminus B = \{g \mid g \in A \text{ and } g \notin B\}$

Note $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and $\overline{A \cap B} = \bar{A} \cup \bar{B}$ via De Morgan's laws.
Other distributive laws exist also.

<u>Quantifiers</u>

$\forall$ = for all

$\exists$ = there exists

$\exists!$ = there exists a unique

$\forall^\infty$ = for all but finitely many

$\exists^\infty$ = there exists infinitely many

?? come up with a formal definition for these in $\mathbb{N}$
$\forall^\infty := \exists n \forall m \geq n$ $\exists^\infty := \forall n \exists m > n$

Subsets

$A \subseteq B$ iff $\forall a \in A,\ a \in B$

$A \subset B$ iff $A \subseteq B$ and $\exists\ b \in B : b \notin A$.

Supersets

As before but with $\supseteq$ and $\supset$.

Power Sets

The power set of a set S is the set of all subsets of S.

Ex) $\mathcal{P}(\mathbb{Z}_2) = 2^{\mathbb{Z}_2} = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$.

fancy P

b/c The power set produces 2^n elements when $|S| = n$.

Tuples

A k-tuple is an ordered list of k things.

Ex) $(0,1,2)$ is a 3-tuple.
(a,b) is a 2-tuple

Cartesian Product

The Cartesian product or cross product of two sets A and B is

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

Sequences

A sequence is and indexed list of objects (like a tuple).

Ex) $000000\ldots$ is an infinite sequence of 0's.

$1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ is an infinite sequence converging to 0.

$abcde\ldots xyz$ is a finite sequence.

Formal Boolean Logic

There are two literals, true and false, usually denoted as either 1 and 0 or T and F respectively.

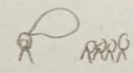
Statements or propositions can be either true or false.

Ex) All horses are the same color.

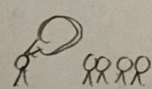
It is raining.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Operations



Disjunction (OR): $P \vee Q$ is true if P or Q is true.
Conjunction (AND): $P \wedge Q$ is true if both P and Q are true.
Negation (NOT): $\neg P$ is true if P is false.
Exclusive Or (XOR): $P \oplus Q$ is true if exactly one of P or Q is true.
Implication: $P \Rightarrow Q$ if when P is true, Q is true.
Equivalence: $P \Leftrightarrow Q$ if $P \Rightarrow Q$ and $Q \Rightarrow P$.
This is often written as iff for "if and only if."

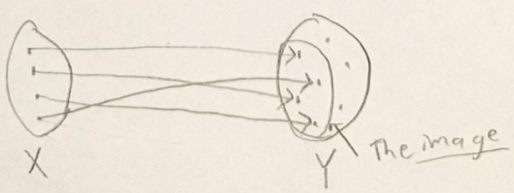


If we have to prove the equivalence of 3 statements, how many things do we have to prove.

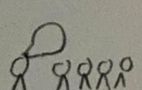
Functions

A function maps inputs from its domain to its codomain or range.

$$f: X \to Y$$



The inverse of a function $f^{-1}: Y \to X$ "undoes" the f operation.



When does the inverse exist?

Surjections (Onto)

A function $f: X \to Y$ is <u>onto</u> if $\forall y \in Y \; \exists x \in X : f(x) = y$.

Injections (one-to-one)

A function $f: X \to Y$ is <u>one-to-one</u> if $\forall x_1, x_2 \in X, \; f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Bijections

A function $f: X \to Y$ is a bijection if it is both surjective and injective.

Note that this is precisely when an inverse function exists.

Relations

A <u>binary relation</u> R between two sets X and Y is a subset of $X \times Y$.

We write $(x, y) \in R$ or $x R y$ to denote x is related to y.

Ex) $<$ is a relation on any set of numbers.
$=$ is too.

A relation R when $X = Y$ is

- <u>reflexive</u> if $\forall x \in X, \; x R x$
- <u>anti-reflexive</u> if $\forall x \in X, \; \neg x R x$
- <u>symmetric</u> if $\forall x, y \in X, \; x R y \Rightarrow y R x$
- <u>anti-symmetric</u> if $\forall x, y \in X, \; x R y \Rightarrow \neg y R x$
- <u>transitive</u> if $\forall x, y, z \in X, \; x R y \wedge y R z \Rightarrow x R z$

A relation which is reflexive, symmetric, and transitive is called an <u>equivalence relation</u>.

Types of Proofs

Direct Proofs (do the math)

Prove that the sum of two even numbers is even.

Let x, y be even.
Then $\exists\, a, b \in \mathbb{Z}$ such that $x = 2a$, $y = 2b$.
Hence $x + y = 2a + 2b = 2(a+b)$.
$\therefore$ $x+y$ is even. □

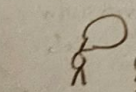
Constructive Proof (show the existence of something)

Prove that $f(x) = x^2$ is not one-to-one.

$f(1) = f(-1) = 1$ □ (counter example proof)

Contradiction Proof

Prove $|\mathbb{N}| < |\mathbb{R}|$.
Clearly $|\mathbb{R}| \geq |\mathbb{N}|$ since $\mathbb{N} \subseteq \mathbb{R}$.
Now suppose that $|\mathbb{N}| = |\mathbb{R}|$.



Then we can enumerate $\mathbb{R}$ as $\{r_n\}_{n \in \mathbb{N}}$ such that $\mathbb{R} = \{r_n \mid n \in \mathbb{N}\}$.
We can write the fractional part of each r_n as

$r_n = d_{1,n} d_{2,n} d_{3,n} d_{4,n} \cdots$

The we can write each r_n together as

$$\begin{array}{cccc} d_{1,1} & d_{2,1} & d_{3,1} & d_{4,1} \cdots \\ d_{1,2} & d_{2,2} & d_{3,2} & d_{4,2} \\ d_{1,3} & d_{2,3} & d_{3,3} & d_{4,3} \\ d_{1,4} & d_{2,4} & d_{3,4} & d_{4,4} \\ \vdots & & & \ddots \end{array}$$

If we define $d_n = \begin{cases} 1 & d_{n,n} \neq 1 \\ 0 & d_{n,n} = 1 \end{cases}$, then $r = d_1 d_2 d_3 d_4 \cdots \in \mathbb{R}$.
But clearly $r \neq r_n$ for any n.
$\rightarrow\leftarrow$ $\therefore |\mathbb{N}| < |\mathbb{R}|$.

□

Contraposition Proofs

Prove $\forall x \in \mathbb{Z}$, x^2 even $\Rightarrow$ x even.

Suppose x is not even. Then x is odd.
The product of two odd numbers is odd, hence $x^2 = x \cdot x$ is odd.
Thus x^2 is not even.

□

Exhaustion Proofs (proof by cases)

Prove that $\forall n \in \mathbb{N}$, $2 \mid 2n^2+n+1 \Rightarrow n$ odd.

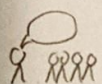
Let $n \in \mathbb{N}$.

Case n odd:
$n = 2a+1$ for some $a \in \mathbb{Z}$
$2(2a+1) + 2a + 1 + 1 = 6a + 4 = 2(3a+2)$

Case n even:
$n = 2a$ for some $a \in \mathbb{Z}$
$2(2a) + 2a + 1 = 6a + 1$

Hence when 2 divides $2n^2+n+1$, n must be odd.

□



What other way(s) could we have divided the cases?

Nonconstructive Proofs

Prove $\exists a, b \in \mathbb{R} \setminus \mathbb{Q} : a^b \in \mathbb{Q}$.

Either $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ and we're done or $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$.

□

Why is this nonconstructive?
We don't ever identify which is correct.

Induction Proofs

Induction takes the general form for a statement P as follows.

$\forall b \in B, P(b)$ where B is a set of base cases.

$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+k)$. (k is usually 1)

Ex) Prove $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

When $n=1$, $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$.

Now suppose $\boxed{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}$. $P(n)$

Then (key to start with n+1)

$$\sum_{k=1}^{n+1} k = n+1 + \sum_{k=1}^{n} k = n+1 + \frac{n(n+1)}{2} = \frac{(n+2)(n+1)}{2}.$$

□

Ex) Prove all horses are the same color.

$P(n)$ = If there are n horses, they all are the same color.

When $n=1$, this is trivial.

Now suppose $P(n)$ is true.

Given n+1 horses, pick 2. Remove one to get a set S of horses and remove the other to get a set R of horses.

Clearly $|S| = |R| = n$, so the horses in S must be all the same color as must all the horses in R.

But since $S \cap R \neq \emptyset$, it follows that all n+1 horses must have the same color.

□

Where does this proof go wrong?

Ex) Prove every amount of postage of at least 12¢ can be made from 4¢ and 5¢ stamps.

WTS $\forall n \in \mathbb{N}, n \geq 12 \; \exists a, b \in \mathbb{N} : n = 4a + 5b$.

When $n = 12$, $a = 3$ and $b = 0$.
When $n = 13$, $a = 2$ and $b = 1$.
When $n = 14$, $a = 1$ and $b = 2$.
When $n = 15$, $a = 0$ and $b = 3$.

Assume true for n.

What do we know about $n+1$?

Instead assume true for $k = 12, 13, \ldots, n-1, n$. (Strong induction)
If $n+1 < 16$, we're done.
Otherwise $n+1 \geq 16$ and hence $(n+1) - 4 \geq 12$.
Thus $\exists a', b' \in \mathbb{N} : (n+1) - 4 = 4a' + 5b'$
Pick $a = a' + 1$ and $b = b'$.
Then $n+1 = 4a + 5b$.

□

Alt) It suffices to show $P(n) \Rightarrow P(n+4)$.
For $n+4$, we know $\exists a', b' \in \mathbb{N} : n = 4a' + 5b'$.
Then $n+4 = 4a' + 5b' + 4 = 4(a'+1) + 5b'$, so pick $a = a'+1$ and $b = b'$.

□

Ex) Prove $\forall x \in \mathbb{R}$, $f(x) = x^2$ is nonnegative.

Define $S_n = [-n, -(n-1)] \cup [n-1, n)$.

Define $P(n) = \forall x \in S_n,\ f(x) \geq 0$.

When $n = 0$, $S_0 = (-1, 1)$. $x^2 \geq 0$

Assume $P(n)$.

Let $x \in S_{n+1}$.

If $x \geq 1$, then $x^2 \geq (x-1)^2 \geq 0$.

If $x \leq -1$, then $x^2 \geq (x+1)^2 \geq 0$.

□