## §2.2

**Def** An argument that establishes the truth of a mathematical statement is called a proof. (I will often abbreviate as pf)

assumptions/hypothesis

conclusion

$p \Rightarrow q$ means if $p$ is true, then $q$ is also true

Ways to prove a statement/claim:

1) direct proof

Ex Claim: For $m, n \in \mathbb{Z}$, if $m$ is odd + $n$ is even, then $m \cdot n$ is even

Pf

Since $m$ is odd
$m = 2k+1$ for some $k \in \mathbb{Z}$

Since $n$ is even, then
$n = 2\ell$ for some $\ell \in \mathbb{Z}$.

Therefore
$$m \cdot n = (2k+1)(2\ell)$$
$$= 2(2k+1)(\ell) \text{, where } \ell(2k+1) \in \mathbb{Z}$$
so $m \cdot n$ is even $\square$

Idea of direct proof:
Assume assumptions stated in claim.
Use existing facts/formulas to prove claim.

2) proof by contradiction

Ex Claim: $\sqrt{2}$ is irrational

Assume $\sqrt{2}$ is rational. If we can reach a contradiction (something false according to our assumptions), we will prove the claim.

If $\sqrt{2}$ is rational, then
$$\sqrt{2} = \frac{p}{q} \text{ for } p, q \in \mathbb{Z} \text{ where } p, q \text{ have no common terms.}$$
$$\Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow p^2 \text{ is even}$$
$$\Rightarrow p \text{ is even}$$
Thus $p = 2k$ for some $k \in \mathbb{Z}$ so
$$2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2 \text{ is even}$$
$$q \text{ is even}$$
$\Rightarrow p, q$ were both multiples of 2 $\rightarrow\leftarrow$ $\square$

Idea of pf by contradiction for $p \Rightarrow q$.
assume $p$ is true + $q$ is false.
Once we reach a contradiction using existing results this proves $q$ is true.

3) Proof by contrapositive.

<u>Ex</u> <u>Claim</u>: Suppose $x \in \mathbb{R}$ is irrational. Then $\sqrt{x}$ is irrational.

Suppose $\sqrt{x}$ is rational. We will show $x \in \mathbb{R}$ is rational.

Then $\sqrt{x} = \frac{p}{q} \Rightarrow x = \frac{p^2}{q^2} \Rightarrow x$ is rational $\square$

Idea of pf by contrapositive of $p \Rightarrow q$

It is a fact that

(opposite of $q$) $\Rightarrow$ (opposite of $p$) is true if and only if $p \Rightarrow q$ is true.

Proving the former claim instead is proof by contrapositive.

4) Proof by cases.

<u>Ex</u> <u>Claim</u>: for each $x \in \mathbb{R}$, $x \leq |x|$.

<u>Case 1</u>: $x \geq 0$
Then $|x| = x$, so $x \leq |x| = x$

<u>Case 2</u>: $x < 0$
Then $|x| > 0$, so $x < 0 < |x|$.

Since this covers all $x \in \mathbb{R}$ and in each case we have proven $x \leq |x|$, we are done

$\square$

Idea of pf by cases of $p \Rightarrow q$

If we can break down $p$ into cases and prove $q$ in each case, we are done.

Other types of proofs:

4) Proving a statement is false.

- Option 1: find a contradiction

Ex) Claim: $m^2$ even $\Rightarrow m$ odd

If $m^2$ even $\Rightarrow m^2 = 2k$
$\Rightarrow m^2 = 4l$ some
$\Rightarrow m = 2\sqrt{l} \Rightarrow m$ even $\rightarrow\leftarrow$

- Option 2: find a counterexample

Ex) Consider $m^2 = 64$.
Then $m = 8$, which is not odd

5) Proving equivalence of statements $p \Leftrightarrow q$ ($p$ if and only if $q$).

For this, we prove

1) $p \Rightarrow q$, and
2) $q \Rightarrow p$

6) Existence proof, i.e. proving the existence of some instance when a statement is true

Ex) Claim: $\{x \in \mathbb{Q} \mid x^3 - 7x^2 + 2x - 14 = 0\} \neq \emptyset$

Factor $(x-7)(x^2+2) \Rightarrow x = 7$ satisfies RHS $\square$

## §2.4

Mathematical Induction:

Ex) Suppose you had a glass of milk last Friday. Every day if you had milk to drink yesterday, you'll also drink milk today.

Q: Will you drink milk today?

A: Yes. From $1^{st}$ statement, you drank milk on the $23^{rd}$. By $2^{nd}$ statement, you also did on 24, 25, 26, 27, 28, 29, ...

**Principle** (Induction) Suppose we have a function of propositions $S(n)$, for $n \in \{n_0, n_0+1, n_0+2, \dots\} \subseteq \mathbb{Z}$

Suppose

(Basis step) 1) $S(n_0)$ is true, and

(Inductive step) 2) For each $n \geq n_0$, if $S(n)$ is true, $S(n+1)$ is true.

Then $S(n)$ is true for each $n \in \{n_0, n_0+1, n_0+2, \dots\}$

Idea: We can prove a statement holds for each $n \in \{n_0, n_0+1, n_0+2, \dots\}$ if we can show

1) It holds for $n = n_0$

2) If it held for previ us $n$, it will hold for next $n$.

Ex) let $S_n = 1 + 2 + \dots + n$ for $n \in \mathbb{Z}_{>0}$

Claim: $S_n = \dfrac{n(n+1)}{2}$ for $n \geq 1$.

Pf

Step 1: basis step

need to show for $n = 1$.

In this case $S_1 = 1 = \dfrac{1(1+1)}{2}$.

Step 2:

Suppose for some $n \geq 1$, $S_n = \frac{n(n+1)}{2}$.

We want to show: $S_{n+1} = \frac{(n+1)(n+2)}{2}$

We know $S_{n+1} = 1 + 2 + \ldots + n + (n+1)$

$$\Rightarrow S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

so by Ind. Principle, we are done!

Ex) (Geometric Sum). For $r \neq 1$,

$$a + ar + ar^2 + \ldots + ar^n = \frac{a(r^{n+1} - 1)}{r-1} \text{ for all } n \geq 0.$$

Basis Step: $n=0$ $\quad a = \frac{a(r^1 - 1)}{r-1}$, so we are done

Ind. step: Suppose true some $n \geq 0$.

Then

$$a + ar + ar^2 + \ldots + ar^n + ar^{n+1}$$

$$= \frac{a(r^{n+1} - 1)}{r-1} + ar^{n+1} = \frac{ar^{n+1} - a + ar^{n+2} - ar^{n+1}}{r-1}$$

$$= \frac{a(r^{n+2} - 1)}{r-1}$$

so by Ind Principle, we are done!

$\boxed{\text{Thm}}$ If $|X| = n$, then $|P(X)| = 2^n$ for all $n \geq 0$.

Pf

Basis Step: $n = 0 \Rightarrow X = \emptyset \Rightarrow P(X) = \{\emptyset\}$

$\Rightarrow |P(X)| = 1 = 2^0$

Ind Step: Suppose true for some $|X| = n$.

Consider $Y$ where $|Y| = n+1$.

Then $Y = Y \setminus \{x\} \cup \{x\}$.

By Ind step, $|P(Y \setminus \{x\})| = 2^n$

We know by the definition of power set,

$P(Y) = P(Y \setminus \{x\}) \cup \{S \in P(Y) \mid x \in S\}$ partitions $P(Y)$

$\Rightarrow |P(Y)| = |P(Y \setminus \{x\})| + |\{S \in P(Y) \mid x \in S\}|$

by Ind Step

$\Rightarrow |P(Y)| = 2^n + |\{S \in P(Y) \mid x \in S\}|$

WTS: $|\{S \in P(Y) \mid x \in S\}| = 2^n$.

It suffices to give a bijection

$f : \{S \in P(Y) \mid x \in S\} \longrightarrow P(Y \setminus \{x\})$

$S \longmapsto S \setminus \{x\}$

$f$ is surjective since if $T \in P(Y \setminus \{x\}) \Rightarrow f(T \cup \{x\}) = T$

$f$ is injective since if $A = B \in P(Y \setminus \{x\})$

$\Longleftrightarrow A \cup \{x\} = B \cup \{x\}$

Thus $2^n = |P(Y \setminus \{x\})| = |\{S \in P(Y) \mid x \in S\}|$

$\Rightarrow |P(Y)| = |P(Y \setminus \{x\})| + |\{S \in P(Y) \mid x \in S\}|$

$= 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$

Ex) Show $5^n - 1 = 0 \mod 4$ for $n \geq 1$

Base Case: $n = 1$ $\quad 5^1 - 1 = 5 - 1 = 4 = 0 \mod 4$, so base case is proven

Inductive Step: Assume for some $n \geq 1$, $5^n - 1 = 0 \mod 4$.

WTS: $5^{n+1} - 1 = 0 \mod 4$.

Note: when $x = a \mod b$ and $y = a \mod b$, we often write $x \equiv y \mod b$

$$5^{n+1} - 1 \equiv 5 \cdot 5^n - 1 \mod 4 = \underline{4 \cdot 5^n + 1 \cdot 5^n - 1} \mod 4$$
$$= 5^n - 1 \mod 4 = 0 \mod 4$$

so we are done

by Ind. Assump.

Ex) Show $2n + 1 \leq 2^n$ for $n = 3, 4, \ldots$

Base Case:
$n = 3$ $\quad 2 \cdot 3 + 1 = 7 \leq 8 = 2^3$, so the base case holds

Ind. Assump:
Suppose for some $n \geq 3$, $2n + 1 \leq 2^n$.

$$2(n+1) + 1 = 2n + 2 + 1 = (2n+1) + 2 \overset{\text{ind assump}}{\leq} 2^n + 2 \overset{\text{for } n \geq 3}{\leq} 2^n + 2^n = 2^{n+1}$$

So the result follows

## 3.1 Functions: brief review

$f: X \to Y$

**Def** $f$ is injective (1-1) if for any $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$, then $x_1 = x_2$.

$f$ is surjective (onto) if for each $y \in Y$, there is some $x \in X$ such that $f(x) = y$

$f$ is bijective if $f$ is both injective + surjective

**Ex** $f: \mathbb{Q} \to \mathbb{Q}$

$x \mapsto 2x - 1$

$f$ is injective:

Pf Suppose $x_1, x_2 \in \mathbb{Q}$ where $f(x_1) = f(x_2)$

$\Rightarrow 2x_1 - 1 = 2x_2 - 1$

$\Rightarrow x_1 = x_2 \Rightarrow f$ is 1-1

$f$ is surjective:

Pf Suppose $y \in \mathbb{Q}$.

WTS there is some $x \in \mathbb{Q}$ such that $f(x) = y$.

We know

$$2x - 1 = y \Leftrightarrow 2x = y + 1 \Leftrightarrow x = \frac{y+1}{2}$$

We know if $y \in \mathbb{Q}$, then $x = y+1/2 \in \mathbb{Q}$.

Therefore taking $x = y+1/2$,

$f(x) = f(y+1/2) = 2(y+1/2) - 1 = y \Rightarrow f$ is onto

Therefore $f$ is 1-1 and onto $\Rightarrow f$ is bijective

**Ex** $f: \mathbb{Z} \to \mathbb{Z}$

$x \mapsto x^2$

$f$ is not injective since $f(1) = f(-1)$ and $1 \neq -1$.

$f$ is not surjective since $-1 \in \mathbb{Z}$ but there is no $x \in \mathbb{Z}$ such that $x^2 = -1$.

$\Rightarrow f$ is not bijective.

§3.2

**Def** A sequence is a function $s : I \to X$ for some set $X$, where $I \subseteq \mathbb{Z}_{\geq 0}$. We write $s_i := s(i)$. $I$ is the domain of $s$.
$i$ ← index of the sequence

If $I$ is finite, we say $s$ is a finite sequence, otherwise, $s$ is infinite.

**Ex)** $s : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ such that $s(i) = 2i$.

Then
$$s_0 = 0$$
$$s_1 = 2$$
$$s_2 = 4$$
$$\vdots$$
$$s_k = 2k$$
$$\vdots$$

If $I = [i, j] = \{i, i+1, \ldots, j-1, j\}$, we write $s$ as $\{s_k\}_{k=i}^{j}$

or if $I = [i, \infty) = \{i, i+1, \ldots\}$, we write $s$ as $\{s_k\}_{k=i}^{\infty}$

need
① $s_k$
② bounds

We call this a closed formula for $s$.

**Ex)** Suppose $s_k = 2^k + 3k$ for each $k \geq 0$.

Then, for example, $s_4 = 2^4 + 6 = 16 + 6 = 22$

**Ex)** Goal: find a closed formula for the sequence $s$:
$$\frac{-1}{3}, \frac{3}{5}, \frac{-5}{7}, \frac{7}{9}, \frac{-9}{11}, \ldots$$

Then $s_k = \dfrac{(-1)^k (2k-1)}{(2k+1)}$ for $k \in \mathbb{Z}_{>0}$

## Properties:

Suppose $i, j \in I$ for $s$. Then we say $s$ is

- increasing if $s_i < s_j$ for each $i<j$
- decreasing if $s_i > s_j$ for each $i<j$
- nonincreasing if $s_i \geq s_j$ for each $i<j$
- nondecreasing if $s_i \leq s_j$ for each $i<j$

Ex) the sequence $\overset{s_1}{5}, \overset{s_2}{6}, \overset{s_3}{12}, \overset{s_4}{81}, \overset{s_5}{4108}$
is increasing & nondecreasing

the sequence $\overset{s_1}{5}, \overset{s_2}{6}, \overset{s_3}{6}, \overset{s_4}{12}, \overset{s_5}{81}, \overset{s_6}{4108}$
is nondecreasing (not increasing since $s_2 = s_3$)

the sequence $\overset{s_1}{5}, \overset{s_2}{6}, \overset{s_3}{-5}, \overset{s_4}{12}, \overset{s_5}{81}, \overset{s_6}{4108}$
is neither (since $s_2 > s_3$ but $s_3 < s_4$)

Def: A subsequence of $s$ is a sequence formed by deleting terms of $s$.

Ex) $\{2k\}_{k=0}^{\infty}$ $\{4k\}_{k=0}^{\infty}$

the latter is a subsequence of the former

Notation: Suppose $n_1, n_2, \ldots$ are the indices of $s$ that correspond to the terms chosen to build the subsequence. Then we use the notation $\{s_{n_k}\}$ to describe the subsequence.

## Operations on $\{s_i\}_{i=k}^{n}$

- addition: $\sum_{i=k}^{n} s_i := s_k + s_{k+1} + s_{k+2} + \dots + s_n$

sigma notation

- multiplication: $\prod_{i=k}^{n} s_i = s_k \cdot s_{k+1} \cdot s_{k+2} \cdot \dots \cdot s_n$

product notation

$i$ is the index
$k$ is the lower limit
$n$ is the upper limit

Ex) Recall the geometric sum

$$a + ar + ar^2 + \dots + ar^n.$$

Can view $s_k = ar^k$ $\quad 0 \le k \le n$
and write $\sum_{k=0}^{n} ar^k$ instead

Def) A **string** is a finite sequence of characters. If the characters all lie in a set $X$, we say the string is over $X$.

The string with no elements is null. The length $|\alpha|$ of a string $\alpha$ is the number of characters in $\alpha$.

The string formed by writing a string $\alpha$ then a string $\beta$ is the concatenation $\alpha\beta$ of $\alpha$ and $\beta$

A substring of $\alpha$ is a string formed by selecting con cutive elements of $\alpha$.

Ex) for $\alpha =$ hamburger

$\beta =$ burge is a substring

$\gamma =$ amber is not a substring

Ex) Define $s_n = 2^n + 4\cdot 3^n$, $n \geq 0$

a) What is $s_0$?

$$s_0 = 2^0 + 4\cdot 3^0 = 1 + 4 = 5$$

b) What is $s_i$, where $i \geq 0$?

$$s_i = 2^i + 4\cdot 3^i$$

c) What is $s_{n-1}$ where $n-1 \geq 0$? $s_{n-2}$ for $n-2 \geq 0$?

$$s_{n-1} = 2^{n-1} + 4\cdot 3^{n-1} \qquad s_{n-2} = 2^{n-2} + 4\cdot 3^{n-2}$$

d) Prove $\{s_n\}_{n=0}^{\infty}$ satisfies

$$s_n = 5 s_{n-1} - 6 s_{n-2} \quad \text{for } n \geq 2.$$

Pf

For $n \geq 2$,
$$\begin{aligned}
5 s_{n-1} - 6 s_{n-2} &\overset{\text{by def of } s}{=} 5\left(2^{n-1} + 4\cdot 3^{n-1}\right) - 6\left(2^{n-2} + 4\cdot 3^{n-2}\right) \\
&= \left(5\cdot 2^{n-1} - 6\cdot 2^{n-2}\right) + \left(5\cdot 4\cdot 3^{n-1} - 6\cdot 4\cdot 3^{n-2}\right) \\
&= \left(5\cdot 2^{n-1} - 3\cdot 2^{n-1}\right) + \left(5\cdot 4\cdot 3^{n-1} - 2\cdot 4\cdot 3^{n-1}\right) \\
&= \left(2\cdot 2^{n-1}\right) + \left(3\cdot 4\cdot 3^{n-1}\right) \\
&= 2^n + 4\cdot 3^n = s_n
\end{aligned}$$

, so the result is proven