§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 $\downarrow$ conclusion $\swarrow$

$$p \Rightarrow q$$

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
$\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where p, q 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.

Ex) Claim: 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.

Ex) Claim: for each $x \in \mathbb{R}$, $x \leq |x|$.

Case 1: $x \geq 0$
Then $|x| = x$, so $x \leq |x| = x$

Case 2: $x < 0$
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, ...

$\boxed{\text{Principle}}$ (Induction) Suppose we have a function of propositions $S(n)$, which runs over $n \in \mathbb{Z}_{>0}$.

Suppose

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

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

Then $S(n)$ is true for each $n \in \mathbb{Z}_{>0}$.

Idea: We can prove a statement holds for each $n \in \mathbb{N}$ if we can show

1) It holds for $n=1$

2) If it held for previous n, it will hold for next n.

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

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

Pf

step 1: basis step

need to show for $n=1$.

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

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 $S_{n+1} = 1 + 2 + \dots + n + (n+1)$

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

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

so by Ind. Principle, we are done!

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

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

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

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

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

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

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,

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

We can give a bijection

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

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

$$f^{-1} : \quad T \cup \{x\} \longleftarrow T$$

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

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

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

§3.2

Def A <u>sequence</u> is a function $s : I \to X$ for some set X. We write $s_i := s(i)$. I is the domain of s.

$I \subseteq \mathbb{Z}_{\geq 0}$

index of the sequence

If I is finite, we say s is a <u>finite sequence</u>, otherwise, s is <u>infinite</u>.

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 $I = [i, j]$, we write s as $\{s_k\}_{k=i}^{j}$

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

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

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

$$s_{k+3} = 2^{k+3} + 3(k+3)$$

Properties:

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

- increasing if $s_i < s_j$
- decreasing if $s_i > s_j$
- nonincreasing if $s_i \geq s_j$
- nondecreasing if $s_i \leq s_j$

Ex) the sequence 5, 6, 12, 81, 4108 is increasing & nondecreasing

the sequence 5, 6, 6, 12, 81, 4108 is nondecreasing

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

Ex) $\{2k\}_{k=0}^{\infty}$ $\{4k\}_{k=0}^{\infty}$ $\{2k\}_{k=0}^{5}$

the latter two are subsequences 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 <u>string</u> 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 <u>null</u>. The <u>length</u> $|\alpha|$ of a string α is the number of characters in α.

The string formed by writing a string α then a string β is the <u>concatenation</u> $\alpha\beta$ of α and β

A <u>substring</u> of α is a string formed by selecting consecutive elements of α.

Ex) for α = hamburger

β = burge is a substring

γ = amber is not a substring