Ch 2. Proofs

§2.1. Mathematical systems, Direct proofs, and counterexamples.

A mathematical system consists of (1) axioms, (2) definitions and (3) undefined terms.

Axioms are assumed to be true.

Definitions are used to create new concepts in terms of existing ones.

Undefined terms are implicitly defined in the axioms.

A theorem is a proposition that has been proved to be true.

A lemma is a theorem that is used to prove another theorem.

A corollary is a theorem that follows easily from another theorem.

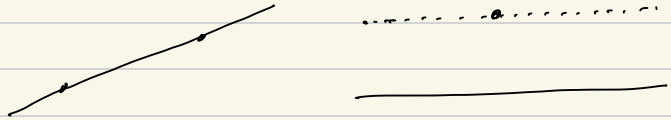
A proof is an argument that establishes the truth of a theorem.

ex) Euclidean geometry.

Axioms : ① Given two distinct points there is exactly one line that contains them.

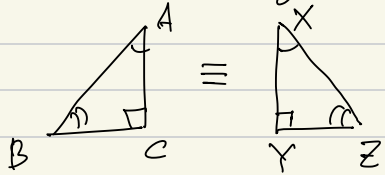
② Given a line and a point not on the line there is exactly one line parallel to the line through the point.

Here, lines and points are undefined terms.



Definitions

- A right triangle is a triangle one of whose angles is 90°.
- Two triangles are congruent if their vertices can be paired so that the corresponding sizes and corresponding angles are the same.



p32 시작해서 axiom 을 사용해 증명

3개가 상대적 개념이지만 엄격하게 구분하기

Theorem (정리) The sum of the angles of a triangle is 180°.

(세 각이 같기에) (정삼각형)

Corollary Every angle of a regular triangle is 60°.

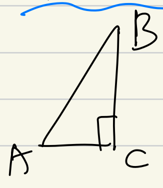
Lemma For every positive integer n, either $n-1$ is a positive integer or $n-1=0$.

* **Direct proofs.** 직접 증명법

A theorem is usually of this form.
For all $x_1, \dots, x_n$, if $p(x_1, \dots, x_n)$ then $q(x_1, \dots, x_n)$.

ex) For every triangle $\triangle ABC$, if $\angle C = 90°$ then $\overline{AB}^2 = \overline{AC}^2 + \overline{BC}^2$.

피타고라스 정리!



A direct proof assumes the given assumption $p(x_1, \dots, x_n)$ and uses axioms, theorems to derive the conclusion $q(x_1, \dots, x_n)$.

Def) An integer n is even if there exists an integer k such that $n = 2k$. An integer n is odd if there is an integer k such that $n = 2k+1$.

ex) 0 is even, $0 = 2 \cdot 0$.
-1 is odd, $-1 = 2(-1)+1$.

Direct proof 예시

Thm For all integers m and n, if m is odd and n is even, then $m+n$ is odd.

pf) Since m is odd, $\exists k \in \mathbb{Z}$, $m = 2k+1$.
Since n is even, $\exists l \in \mathbb{Z}$, $n = 2l$.
Then $m+n = (2k+1)+(2l)$
$= 2\underbrace{(k+l)}_{\in \mathbb{Z}} + 1$

$\therefore m+n$ is odd. □

end of proof. → Q.E.D.

여러개의 증명법 존재

There can be many proofs of one theorem.

Thm For all sets X and Y, $X \cup (Y-X) = X \cup Y$.
($\subseteq$ and $\supseteq$)

Pf 1) We need to show ① $X \cup (Y-X) \subseteq X \cup Y$
② $X \cup (Y-X) \supseteq X \cup Y$.

① Let $x \in X \cup (Y-X)$.
Then $x \in X$ or $x \in Y-X$.
If $x \in X$, then $x \in X \cup Y$.
If $x \in Y-X$, then $x \in Y$, so $x \in X \cup Y$.
So, $x \in X \cup Y$.

② Let $x \in X \cup Y$.
If $x \in X$, then $x \in X \cup (Y-X)$.
If $x \notin X$, then we must have $x \in Y$
Then $x \in Y-X$. $\Rightarrow$ $x \in X \cup (Y-X)$.
So $x \in X \cup (Y-X)$. □

Pf 2) Let U be a universe containing X, Y.

$X \cup (Y-X) = X \cup (Y \cap \bar{X})$ ($Y-X = Y \cap \bar{X}$)
$= (X \cup Y) \cap (X \cup \bar{X})$ (distributive law)
$= (X \cup Y) \cap U$ (complement law)
$= X \cup Y$ (identity law) □

반증하다

* Disproving a statement.
In order to disprove $\forall x\, P(x)$, we need to find x such that $P(x)$ is false.

ex) $\forall n \in \mathbb{Z}^+$ (2^n+1 is prime)
If $n=3$, then $2^n+1 = 2^3+1 = 8+1 = 9$, not prime.
So the statement is false. □.

참인지 같으면 prove, 거짓인지 같으면 disprove

ex) Prove or disprove: $\forall$ sets A, B, C,
$(A \cap B) \cup C = A \cap (B \cup C)$
sol) Let $A = B = \emptyset$, $C = \{1\}$.
$(A \cap B) \cup C = \{1\}$.
$A \cap (B \cup C) = \emptyset$] different
False. □.

§2.2. More methods of proofs.

* Proof by contradiction.

A proof by contradiction 무모 is a proof technique to prove $p \to q$ by assuming p and $\neg q$ and deriving a contradiction.

(A contradiction is a statement of this form $r \wedge \neg r$.)

Since $\neg q$ cannot happen (False), we must have q.

This is an indirect proof. 간접 증명법

ex) $\forall n \in \mathbb{Z}$, if n^2 is even then n is even.

Pf) Suppose n^2 is even but n is odd.

Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

$n^2 = (2k+1)^2 = 4k^2+4k+1$

$= 2(2k^2+2k)+1$: odd.

This is a contradiction to the assumption that n^2 is even.

Thus if n^2 is even then n is even. □

ex) $\forall x, y \in \mathbb{R}$, if $x+y \geq 2$ then $x \geq 1$ or $y \geq 1$.

결론을 부정의 가정과 결론을 부정하지 않았으므로

Pf) Suppose $x+y \geq 2$ but $x < 1$ and $y < 1$.

Then, since $x<1$, $y<1$, we have $x+y<2$.

This is a contradiction.

Thus if $x+y \geq 2$, then $x \geq 1$ or $y \geq 1$. □

ex) $\sqrt{2}$ is irrational. 무리수

Pf) Suppose that $\sqrt{2}$ is rational. Then $\exists\, a, b \in \mathbb{Z}$ s.t. $\sqrt{2} = \frac{a}{b}$. 유리수

We may assume that a and b have no common factors. (If they have, we can divide a and b by their greatest common divisor.) 서로소이다.

Then $a = \sqrt{2}\, b$. $\Rightarrow a^2 = 2b^2$.

Then $a = 2k$ for some $k \in \mathbb{Z}$.

Then $(2k)^2 = 2b^2 \Rightarrow 4k^2 = 2b^2$

$\Rightarrow b^2 = 2k^2$. $\Rightarrow b = 2l$, $l \in \mathbb{Z}$.

Then a and b have a common factor 2, which is a contradiction.

$\Rightarrow \sqrt{2}$ is irrational. □

* Proof by cases (Exhaustive Proof).
철저한

This technique divides the assumption into all possible cases and prove each case.
각 경우마다

ex) Prove that $2m^2+3n^2=40$ has no solutions in positive integers.

Pf) Since $2m^2 \le 2m^2+3n^2 = 40$, (n이 최소)

$m^2 \le 20. \Rightarrow m \le 4.$

Since $3n^2 \le 2m^2+3n^2 = 40$, (m이 최소)

$n^2 \le 13.xxx \Rightarrow n \le 3.$

Therefore (m, n) is one of the following.

~~(1,1)~~, ~~(1,2)~~, ~~(1,3)~~
~~(2,1)~~, ~~(2,2)~~, ~~(2,3)~~
~~(3,1)~~, ~~(3,2)~~, ~~(3,3)~~
~~(4,1)~~, ~~(4,2)~~, ~~(4,3)~~.

one by one check

$2\cdot 1^2+3\cdot 1^2 = 5 \ne 40$

$2\cdot 1^2+3\cdot 2^2 = 2+12 = 14 \ne 40$

⋮

None of these satisfies $2m^2+3n^2=40$.

So there are no pos. int. sol. (no solution) □.

* Proof of equivalence.
동치

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p).$

To prove " p if and only if q"

we show two things : $p \to q$ and $q \to p$. (이걸 증명하면 됨)

(if and only if → iff)

ex) $\forall n \in \mathbb{Z}$, n is odd iff $n-1$ is even.

Pf) ($\Rightarrow$) Since n is odd, $n = 2k+1$, $k \in \mathbb{Z}$.

Then $n-1 = (2k+1)-1 = 2k$: even.

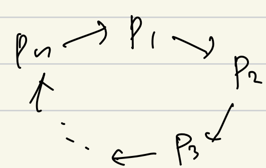
($\Leftarrow$) Since $n-1$ is even, $n-1 = 2k$, $k \in \mathbb{Z}$.

Then $n = (n-1)+1 = 2k+1$: odd. □.

In order to show the equivalence of several propositions $p_1, p_2, \dots, p_n$, we can show

$(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n) \wedge (p_n \to p_1).$

어느 2개의 P를 골라도 $P_i \longleftrightarrow P_j$ 성립



ex) Let A and B be sets.
Prove that TFAE (the following are equivalent).
(a) $A \subseteq B$ (b) $A \cap B = A$ (c) $A \cup B = B$

Pf) (a)→(b): Let $x \in A \cap B$. Then $x \in A$.
Let $x \in A$. By assumption (a), we have $x \in B$.
So $x \in A \cap B$. → ① $A \cap B \subseteq A$ ② $A \cap B \supseteq A$ ⇒ =

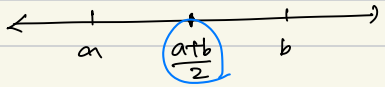
(b)→(c): $x \in A \cup B$. Then $x \in A$ or $x \in B$.
If $x \in A$ then by (b), $x \in A \cap B$, so $x \in B$.
Now let $x \in B$. Then $x \in A \cup B$.

(c)→(a): Let $x \in A$.
Then $x \in A \cup B = B$. Hence $A \subseteq B$. □.

$x \in A \to x \in B$ True ; $A \subseteq B$

* Existence Proof.
$\exists x\, P(x)$ can be proved by exhibiting one example of x s.t. $P(x)$ is true.

ex) $\forall a, b \in \mathbb{R}$, if $a<b$, then $\exists x \in \mathbb{R}$, $a<x<b$.
Pf)



Let $x = \frac{a+b}{2}$. Then $a<x<b$.
$\because x-a = \frac{a+b}{2} - a = \frac{b-a}{2} > 0 \Rightarrow x > a$
$b-x = b - \frac{a+b}{2} = \frac{b-a}{2} > 0 \Rightarrow b > x$.

ex) Let $A = \frac{s_1+\cdots+s_n}{n}$. Prove that there is i s.t. $s_i \geq A$.

Pf) Suppose that the conclusion is false.
Then $s_i < A$ for all $i = 1, \ldots, n$.
Then $s_1+s_2+\cdots+s_n < \underbrace{A+\cdots+A}_{n} = nA$.

$\frac{s_1+\cdots+s_n}{n} < A$, contradiction.

So there must be i s.t. $s_i \geq A$. □.

Such a proof is called "a non-constructive proof."

§2.4. Mathematical Induction. 수학적 귀납법 / 증명기법

The mathematical induction is a proof technique to prove a statement $\forall n \in \mathbb{Z}^+, S(n)$ by showing

① $S(1)$ is true (Basis step)

② For all $n \geq 1$, if $S(n)$ is true, then $S(n+1)$ is also true. (Inductive step).

$\forall n$, $S(n)$: $S(1), S(2), S(3), S(4), \ldots$ $S(n)$ True!

T T T T

Def) For $n \geq 0$ integer,

$$n! = \begin{cases} 1 & \text{if } n=0 \\ 1 \cdot 2 \cdots n & \text{if } n \geq 1. \end{cases}$$

ex) Prove that $n! \geq 2^{n-1}$ for all $n \geq 1$.

pf) Basis step : If $n=1$, then

$1! = 1 \geq 2^{1-1} = 2^0 = 1$.

True for $n=1$.

Inductive Step : Suppose that the statement is true for $n \geq 1$. Then $n! \geq 2^{n-1}$ assumption

$$\begin{aligned} (n+1)! &= n!\,(n+1) \\ &\geq 2^{n-1}(n+1) \quad \text{(by induction hypothesis)} \\ &\geq 2^{n-1} \cdot 2 = 2^n. \end{aligned}$$

So the statement is also true for $n+1$.

By induction, $n! \geq 2^{n-1}$ for all $n \geq 1$. □.

If we want to show that $S(n)$ is true for all integers $n \geq n_0$ (for some fixed n_0), we can also use induction. 임의의 정수

Basis step : $S(n_0)$ is true.

Induction step : For $n \geq n_0$, if $S(n)$ is true then $S(n+1)$ ..

(a is divisible by b means $a = bk$ for some $k \in \mathbb{Z}$).

ex) Let $a, r \in \mathbb{R}$, $r \neq 1$.
Prove that $a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1}-1)}{r-1}$.
for all integers $n \geq 0$.

Pf) Basis step: $n = 0$.
$LHS = a$, $RHS = \frac{a \cdot (r^1 - 1)}{r-1} = a$.
True.
Inductive Step: Suppose it's true for $n \geq 0$.
Then $a + ar + \cdots + ar^n = \frac{a(r^{n+1}-1)}{r-1}$.

$a + ar + \cdots + ar^n + ar^{n+1} = \frac{a(r^{n+1}-1)}{r-1} + ar^{n+1}$
Induction hypothesis.

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

True for $n+1$.
By Induction, true for all $n \geq 0$. □

ex) Prove that $5^n - 1$ is divisible by 4
for all $n \geq 0$.

Pf) Basis step: If $n = 0$, then $5^0 - 1 = 1 - 1 = 0$.
is divisible by 4. $(0 = 4 \cdot 0)$.

Ind Step: Suppose it's true for $n \geq 0$.
Then $5^n - 1 = 4k$, $k \in \mathbb{Z}$.
$5^{n+1} - 1 = 5 \cdot 5^n - 1$
$= 5 \cdot (5^n - 1 + 1) - 1$
$= 5(4k+1) - 1$
$= 20k + 4$
$= 4(5k+1)$ is div by 4.
True for $n+1$.
By Ind, true for all $n \geq 0$. □

Thm X: a set.
If $|X|=n$, then $|P(X)|=2^n$.
for all $n \geq 0$.

Pf) If $n=0$, then $X=\emptyset$, hence $P(X)=\{\emptyset\}$.
So $|P(X)| = 1 = 2^0$. True!

Suppose that the statement is true for $n \geq 0$.
Suppose $|X| = n+1 \geq 1$.
Let $x \in X$ and $Y = X - \{x\}$.
Then $|Y| = n$.
$|P(X)|$ = (# subsets of X)
= (# subsets of X containing x) ①
+ (# " not containing x) ②

Since $A \subseteq X$, $x \in A \iff A = B \cup \{x\}$
for some $B \subseteq Y$,
① = (# subsets of Y) $= 2^n$

Since $A \subseteq X$, $x \notin A \iff A \subseteq Y$.
② = (# subsets of Y) $= 2^n$.

So $|P(X)| = ① + ② = 2^n + 2^n = 2^{n+1}$.
So, also true for $n+1$.
By Ind, true for all $n \geq 0$. □

§2.5. Strong form of Induction and the well-ordering property.

A strong form of Induction (or strong induction) is a proof technique to prove $\forall n \geq n_0, S(n)$ by showing

① Basis step : $S(n_0)$ is true

② Inductive step : If $S(k)$ is true for all $n_0 \leq k < n$, then $S(n)$ is true.

Comparison between Ind & strong Ind.

Ind : $n_0, n_0+1, n_0+2, \ldots, n, n+1$

Strong Ind : $n_0, n_0+1, n_0+2, \ldots, n, n+1$

$n_0 \to n_0+1$ 증명

$n_0, n_0+1 \to n_0+2$ 증명

$n_0, n_0+1, n_0+2 \to n_0+3$ 증명 (이런 느낌)

ex) Show that postage of 4 cents or more can be achieved by using only 2-cent and 5-cent stamps.

Pf) Strong Ind on n $(n \geq 4)$.

Basis step : $n=4=2+2$, $n=5=5$) true.

Ind step : Suppose that it is true for all k with $4 \leq k < n$ $(n \geq 6)$.

We consider n $(n \geq 6)$.

Then $n = 2+(n-2)$. n 사용 X, $n-2$ 사용 (이전까지 증명한 귀납가정)

Since $4 \leq n-2 < n$, by Ind hyp

$n-2 = 2 \cdot a + 5 \cdot b$ for some $a, b \in \mathbb{Z}_{\geq 0}$.

Then $n = 2+(2a+5b)$

$= 2(a+1)+5b$.

So it's also true for n.

By strong Ind, true for all $n \geq 4$. □

ex) For $n \geq 1$, c_n is defined by

$c_1 = 0$, $c_n = c_{\lfloor n/2 \rfloor} + n$ for $n \geq 2$.

Prove that $c_n < 2n$ for all $n \geq 1$.

Pf) Strong Ind on n.

$n = 1$: $c_1 = 0 < 2$ True.

Suppose it is true for all $1 \leq k < n$ $(n \geq 2)$.

Then $c_n = c_{\lfloor n/2 \rfloor} + n$ $(1 \leq \lfloor n/2 \rfloor < n)$

$\leq 2\lfloor n/2 \rfloor + n$ (by Ind hyp)

$\leq 2 \cdot n/2 + n$

$= n + n$

$= 2n$.

True for n.

By strong ind, true for all $n \geq 1$. □

자연수 정렬성

* Well-ordering Property. 음이 아닌 정수의

Every nonempty set of nonnegative integers has a least element.

(This is equivalent to Induction.)

왜냐?

$\{1, 2, 3, \ldots\}$: min = 1

$\{2, 4, 6, \ldots\}$: min = 2.

음이 아닌 정수 = 왼쪽으로 끝이 정해짐

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

does not have a least.

Thm (Quotient-Remainder Theorem).
d, n : integers. $d>0$.
Then there exist unique integers q, r
s.t. $n = dq + r$, $0 \le r < d$.

(q: quotient, r: remainder)

ex). $n=42$, $d=5$.
$42 = 5 \cdot 8 + 2$. $0 \le 2 < 5$.

Pf of Thm
Let $X = \{ n - dk \mid k \in \mathbb{Z},\ n - dk \ge 0 \}$.
Then $X \neq \emptyset$. (not empty)
(∵ If $n \ge 0$, then $n = n - d \cdot 0 \ge 0$. ($k=0$ 가정)
So, $n \in X$.
If $n<0$, then $n - dn = (1-d)n \ge 0$. ($k=n$ 가정)
($1-d \ge 0$, $n<0$)
So, $n - dn \in X$.)
By well-ordering property, X has a least elt.
Let $r = \min X$.
Then since $r \in X$, we can write
$r = n - dq$ for some $q \in \mathbb{Z}$.
Then $n = dq + r$, and $r \ge 0$.
Suppose $r \ge d$. Then
$0 \le r - d = (n - dq) - d = n - d(q+1)$.
So, $r - d \in X$. But this is a contradiction
to $r = \min X$. ($r - d < r$).
Therefore, $r < d$. (가정이면 False)
So, $0 \le r < d$ as desired.

It remains to show that q and r are unique.
Suppose $n = dq' + r'$, $0 \le r' < d$.
Then $r - r' = (n - dq) - (n - dq') = d(q' - q)$.
Since $0 \le r, r' < d$, we have
$-d < r - r' < d$. (r, r' 정수이므로 $-1 \le r - r' \le 1$)
Since $r - r'$ is divisible by d, $r - r' = 0$.
Thus $r = r'$.
Then $0 = d(q' - q) \Rightarrow q' - q = 0 \Rightarrow q' = q$. ($d \neq 0$)
Therefore r and q are the unique integers satisfying the conditions. □