Lecture 7

Proofs of Theorems. Sect. 1.4, 1.5.

$\mathbb{N}$ - natural number.

Theorem 1 If $n = a^2 - b^2$ then either n is odd ($2 \nmid n$) or $4 \mid n$.

P - "$n = a^2 - b^2$".

Q_1 - "n is odd"

Q_2 - "$4 \mid n$".

Theorem. $P \Rightarrow (Q_1 \vee Q_2)$.

$\Leftrightarrow (P \Rightarrow Q_1) \vee (P \Rightarrow Q_2)$.

Proof. Analysis. $a^2 - b^2 = (a+b)(a-b)$. $\tilde{P}$: $n = (a+b)(a-b)$

Theorem P_1. For any a, b the numbers $a+b$, $a-b$, either both even or both odd.

R_1 "$a+b$ is even";

P_{1n} "$a-b$ is even"

Theorem. $(R_1 \wedge R_2) \vee (\sim R_1 \wedge \sim R_2)$.

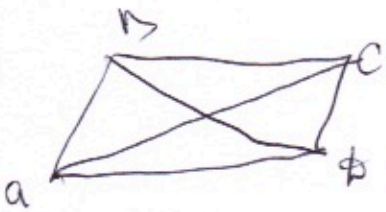
Proof. Corrolary of Theorem on sums and differences of odd and even num

Theorem P_2. Product of odd numbers is odd and product of even numbers is multiple 4.

$$\tilde{P} \wedge P_1 \wedge P_2 \Rightarrow Q_1 \vee Q_2,$$

Some Theorems it's convenient to reduce to conditional.

Theorem. If at parallelogram $\square ABCD$ the diagonals $AC = BD$ then it's a rectangle ($\angle BAD$ is right).



P_1 — $\square ABCD$ is a parallelogram

P_2 — $AC = BD$

Q — $\angle BAD = 90^\circ$

Theorem. $P_1 \wedge P_2 \Rightarrow Q$.

Analysis. $\triangle ADD = \triangle ACD$ on SSS.

~~Theorem.~~ Theorem. $P_1 \Rightarrow P_3$ is true.
P_3: $AB = CD$

Specialization of Theorem on opposite sides of parallelograms.

P_4 — " AD is an joint side of $\triangle ABD$ and $\triangle ACD$, "

P_5 — " $\triangle ABD = \triangle ACD$.

$P_2 \wedge P_3 \wedge P_4 \Rightarrow P_5$ — True on SSS Then

So P_5 is True.

$P_5 \Rightarrow P_6$

~~$\triangle ABD \cong \triangle CDA$~~ $\angle BAD = \angle CDA$ (angles opposite to the ~~diagonals~~ diagonals).

$P_1 \Rightarrow P_7$ ($\angle BAD + \angle CDA = 180^\circ$)

$P_6 \wedge P_7 \Rightarrow Q.$ ☒

Proof by Contraposition (or by Reduction to Contradiction).

The original version follows to

$$(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P).$$

So we can apply modus ponens to 2nd conditional $\sim Q \Rightarrow \sim P$.

The other other equivalent forms.

Most convenient

$$(P \Rightarrow Q) \Leftrightarrow (P \wedge \sim Q) \Rightarrow (F)$$

So if we suppose that P and $\sim Q$ both True and receive any Contradiction (F) (indentical Lie).

We'll try to understand how to prove Theorems

- analyse specific mathematical proofs (1)
- analyse logical tools (2)
- solve problems on proofs (3)

Properties of convolution can be useful

Proposition: Next connectives are equivalent to Convolution $P \Rightarrow Q$

(i) $\sim Q \Rightarrow \sim P$; (contraposition)

(ii) $(P \wedge \sim Q) \Rightarrow \sim P$;

(iii) $(P \wedge \sim Q) \Rightarrow Q$;

(iv) $(P \wedge \sim Q) \Rightarrow F$

↑ Contradiction (any identical False), i.e. Pm

- How to prove these equivalencies?

- How to use them?

Examples.

Theorem. $\sqrt{2}$ is an irrational.

Formalization of the statement.

There are no such natural m, n that $2m^2 = n^2$. $\quad 2 = \frac{n^2}{m^2}$. $\quad \neg Q$

Proof. Let suppose such m, n exist and (m, n) have no joint divisor $\neq 1$.

$(2m^2 = n^2) \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n \Rightarrow 4 \mid n^2 \Rightarrow 2 \mid n^2$

$\neg Q \quad \Rightarrow 2 \mid m \Rightarrow$ 2 is an joint divisor for m and n.

Contradiction. ∎

Theorem. There are infinitely many different prime numbers.

Proof. ~ Q

Let the set of prime numbers is $p_1, p_2, p_3, \ldots, p_k$ are all prime numbers

Let us consider

$$n = p_1 \cdots p_k + 1.$$

R_1 - $n > p_j$ for all j $\Rightarrow$ R_2 - n is not prime

R_3 $p_j \nmid n$ for all j since $p_j \mid (n-1)$, and $n, n-1$ can't have join factors $\neq 1$.

$\Rightarrow \exists R_2$

Contradiction

We define $P \Rightarrow Q$ by its True Table:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The table follows to the principle
« From Truth follows only Truth
but from Lie can follow both
Truth and Lie. »

Properties:

1. $P \Rightarrow Q \equiv \sim P \vee Q$
2. $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$
3. $P \Rightarrow (Q \Rightarrow R) \equiv (P \wedge Q) \Rightarrow R$
4. $P \Rightarrow (Q \wedge R) \equiv (P \Rightarrow Q) \wedge (P \wedge R)$
5. $(P \vee Q) \Rightarrow R \equiv (P \Rightarrow R) \wedge (Q \Rightarrow R)$.

True tables or narratives.