Lecture 8.
Proofs (continuation).  Sect. 1.5, 1.6, 1.7

1. Quiz 3:

2. Selected problems from HA 4.

Sect. 1.4
Pr. 4 (a)

Elem.

\[ P_3 \quad \text{Plum is guilty} \]

\[ P_2 \quad \text{Crime in kitchen} \]

\[ \neg P_2 \quad \text{at midnight} \]

\[ P_3 \quad \text{By weapon - candlestick} \]

\[ P_5 \quad \text{Crime in library} \]

(i) \( \neg P_1 \Rightarrow P_2 \)
(ii) \( P_2 \Rightarrow P_4 \)
(iii) \( P_4 \Leftrightarrow \neg P_4 \)
(iv) \( (P_4 \land \neg P_5) \lor (P_5 \land \neg P_5) \) - alternative disjunction
(v) \( \neg P_4 \) - Scarlet is guilty
(a) \( P_5 \Rightarrow \neg P_2 \Rightarrow P_3 \)  
(b) \( \neg P_5 \Rightarrow \neg P_4 \Rightarrow P_3 \)  
(c) \( \neg P_3 \land \neg P_4 \Rightarrow P_1 \land P_5 \)  
(d) \( P_3 \Rightarrow P_1 \)  

<table>
<thead>
<tr>
<th></th>
<th>Criminal</th>
<th>Place</th>
<th>Time</th>
<th>Weapon</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Plum</td>
<td>Library</td>
<td>?</td>
<td>Revolver</td>
</tr>
<tr>
<td>b</td>
<td>Phoebe</td>
<td>Kitchen</td>
<td>?</td>
<td>Poisons, Candelstick</td>
</tr>
<tr>
<td>c</td>
<td>Plum</td>
<td>Library</td>
<td>12PM</td>
<td>Revolver</td>
</tr>
<tr>
<td>d</td>
<td>Plum</td>
<td>Conserv.</td>
<td>12PM</td>
<td>Revolver</td>
</tr>
</tbody>
</table>
Exercises 1.4

1.4 Basic Proof Methods

I. Analyze the logical form of each of the following statements and determine

\[ \exists x P(x) \land \neg \exists y Q(y) \]

2. Assume the premises are true, prove the conclusion.

\[ \neg P(0) \land \exists x P(x) \rightarrow \quad \exists x P(x) \land \neg \exists y Q(y) \]

3. Repeat Exercise 2 assuming the interpreting domain is empty.

\[ \neg P(0) \land \exists x P(x) \rightarrow \quad \exists x P(x) \land \neg \exists y Q(y) \]

4. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \exists x P(x) \), then \( \exists y R(y, 6) \).

5. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \neg \exists x P(x) \), then \( \exists y R(y, 6) \).

6. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \exists x P(x) \land \neg \exists y Q(y) \), then \( \exists z R(z, 7) \).

7. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \neg \exists x P(x) \land \exists y Q(y) \), then \( \exists z R(z, 7) \).

8. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \exists x P(x) \land \exists y Q(y) \), then \( \exists z R(z, 7) \).

9. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \neg \exists x P(x) \land \neg \exists y Q(y) \), then \( \exists z R(z, 7) \).

10. Let the universe be the set of integers and the predicate symbols be defined as follows:

- \( P(x) \) for "\( x \) is even",
- \( Q(x) \) for "\( x \) is prime",
- \( R(x, y) \) for "\( x \) divides \( y \)."

Prove that if \( \exists x P(x) \land \neg \exists y Q(y) \), then \( \exists z R(z, 7) \).
5i) \( x = 2m, y = 2m+1 \Rightarrow xy = 4mn + 2m + 1 = 2(2mn + m) + 2 \Rightarrow xy \text{ is even.} \)

7i) \( \mathbb{Z} \)-integer numbers

\[ a > 0 \land b > 0 \land (a b = 1) \Rightarrow a \leq 1 \land b \leq 1 \Rightarrow 0 < a < 1 \land 0 < b < 1 \Rightarrow a = b = 1. \]

7b) \( a b c \not\equiv c = abq \Rightarrow aqc \)

\( a \mid b \Leftrightarrow b = aq \text{ for some } q \in \mathbb{Z} \)

8a) \( \forall n \in \mathbb{N} \Rightarrow n^2 + n + 3 \text{ odd} \)

2 cases: \( n \text{ - odd } \lor n \text{ - even} \)

\( h = 2k+1 \Rightarrow h^2 + n = (\text{odd}) + (\text{odd}) = \text{even} \)

\( h = 2k \Rightarrow h^2 + n = (\text{even}) + (\text{even}) = \text{even} \)

\( h^2 + n + 3 \text{ - odd as a sum of even and odd} \)

9a) \( \frac{x+y}{2} > \sqrt{xy} \Leftrightarrow \frac{(x+y)^2}{4} > xy \)

\( \forall x, y > 0 \) since \( x > 0, y > 0 \)

\( x > 0, y > 0 \) \text{ Theorem. } a \geq b

Theorem: \( (a > 0 \land b > 0) \Rightarrow (a \geq b \Leftrightarrow a^2 \geq b^2) \)
\[
\frac{x^2 + y^2 + 2xy}{4} \geq xy \Leftrightarrow (x-y)^2 \geq 0,
\]

9d) \(x^3 + 2x^2 < 0 \Rightarrow 2x + 5 < 1\)
\[x^2(x+2) < 0 \Leftrightarrow x < 0 \land x+2 < 0 \Leftrightarrow x < -2\]
\[\Rightarrow 2x + 5 < 1\]

1.5. 3y) \& x \neq 1 \Rightarrow \alpha - even.
\[P \Rightarrow Q\]

Contraposition: \(\sim Q \Rightarrow \sim P\).

Let \(\sim Q \) be True: \(x\) is odd: \(x = 2k + 1\)
\[\Rightarrow x^2 - 1 = 4k^2 + 4k = 4k(k+1)\]
(\(k\)-even \(v\) even-odd)
\[P_1: x = 2k + 1 \land k(k+1)\]
\[(P_1 \land \sim Q) \Rightarrow 8|2k^2 - 1\], Contradiction.

9d. \(xy\) - even \(\Rightarrow x\)-even \(v\) y-even
\[P \Rightarrow Q, \sim Q \Rightarrow y^2\]

\(\sim Q: x = 2k + 1 \land y = 2k + 1 \Rightarrow xy \)-odd \((\sim P)\).
Extra Problems.

1. \(a_i\) - # of handshakes of \(i\)-th person.

\[ A = a_1 + \ldots + a_n. \]

If \(B\) - the number of all handshakes then \(A = 2B.\)

(2 persons at each handshake).

\[ A = A_{\text{even}} + A_{\text{odd}} \]

Every sum of h.s. for people with even h.s.

\[ A_{\text{odd}} \]

\[ A_{\text{even}} \times A_{\text{even}} \rightarrow A_{\text{odd}} \text{ is even.} \]

\[ A_{\text{odd}} \] - the sum of odd numbers \(\Rightarrow\) the number of these numbers (people) is even.
2. Theorem. Let a rectangular $ABCD$ diagonal $AC = BD$.

Let $P = P_1 \cap P_2$, $P_1 \rightarrow \text{Parallelogram}$

$P_1 - \square ABCD - \text{parallelogram}$
$P_2 \angle BAC = \angle ADC - \text{right}$.

Key idea: Consider right triangles $ABD$ and $ACD$.

Proof: 1) Intermediate proposition

$R_2 \Rightarrow S$

Corresponding legs at right triangles are equal $R$  
$\Rightarrow$ triangles are congruent. $S$

2) $P_1 \Rightarrow P_2 - \text{opposite sides are equal}$

Specialization of $R_1$: Even $AB = CD$, $R_2 - \text{AD is joint}$

3) $R = R_1 \cap R_2 \Rightarrow T \Rightarrow S$.

4) $S \Rightarrow \text{hypotenuses are equal (} AC = BD \text{)}$.
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 in practice.

Propositions: Next connectives are equivalent to convolution \( P \Rightarrow Q \)

(i) \( \sim Q \Rightarrow \sim P \) ; (contraposition)
(ii) \( (P \land Q) \Rightarrow P \) ;
(iii) \( (P \land \sim Q) \Rightarrow Q \) ;
(iv) \( (P \land \sim Q) \Rightarrow \sim P \) ;

- How to prove these equivalences?
- How to use them?
Examples.

Theorem. \( \sqrt{2} \) is an irrational.

Formalization of the statement.

There are no such natural \( \& m, n \) that \( 2m^2 = n^2 \).

\[ 2 = \frac{n^2}{m^2} \]

Proof. Let such \( m, n \) exist. No joint divisor \( \neq 1 \).

\((2m^2 = n^2) \Rightarrow 2|n^2 \Rightarrow 2|n \Rightarrow 4|n^2 \Rightarrow 2|m^2 \Rightarrow 2 \text{ is a joint divisor for } m \text{ and } n. \]

Contradiction.
Theorem. There are infinitely many different prime numbers.

Proof. Let the set of prime numbers is $P_1, P_2, P_3, \ldots, P_n$ are all prime numbers.

Let us consider $h = P_2 \cdots P_n + 1$.

$R_1$: For all $j$, $h > P_j$.

$R_2$: $h$ is not prime.

$R_3$: $P_j$ divides $h$ for all $j$ since $P_j | (h-1)$, and $h, h-1$ can't both be prime.

$\Rightarrow \exists R_2$ Contradiction.
Division with a remainder.

Let \( a, b \in \mathbb{Z} \)

\[ b = aq + r, \quad \text{where } 0 \leq r < |a|. \]

\( q \) - quotient, \( r \) - remainder.

Simple problems.

1. For \( b \in \mathbb{N}, a = 6 \), the remainder in the division on 6 is equal 5.
   What will be the remainder in the division \( a \) on 3?

2. Which remainders are possible in the division \( b = h^2 \) on 5?

   **Hint:** It's enough to consider \( h = 0, 1, 2, 3, 4 \)

   \[ h = 5k + r, \quad h^2 = (5k+r)^2. \]