Summary on Lecture 5, January 23, 2019

- **Logical equivalence.** Recall that two propositions \( s_1 \) and \( s_2 \) are logically equivalent if \( s_1 \) is true if and only if \( s_2 \) is true. We use the notation: \( s_1 \iff s_2 \)

  Examples:

  (a) \( (p \to q) \iff (\neg p \lor q) \)

  (b) \( (p \to q) \iff (\neg q \to \neg q) \)

- **The Laws of logic.**

  1. \( \neg \neg p \iff p \)  
     (Double negation)
  2. \( \neg (p \lor q) \iff (\neg p \land \neg q) \)
     (DeMorgan Laws)
  3. \( (p \lor q) \iff (q \lor p) \)  
     (Commutativity Laws)
  4. \( (p \lor q) \lor r \iff p \lor (q \lor r) \)
     (Associativity Laws)
  5. \( [p \lor (q \land r)] \iff [(p \lor q) \land (p \lor r)] \)
     (Distributive Laws)
  6. \( p \land p \iff p \)
     (Idempotent Laws)
  7. \( p \lor F_0 \iff p \)
     (Identity Laws)
  8. \( p \land T_0 \iff p \)
     (Inverse Laws)
  9. \( p \land \neg F_0 \iff F_0 \)
     (Domination Laws)
 10. \( p \lor (p \land q) \iff p \)
     (Absorption Laws)
 11. \( p \land (p \lor q) \iff p \)

  (a) Show that the implication \( [p \land (p \to q)] \to q \) is a tautology.

  (b) Show that \( (p \to q) \iff (p \land q) \) is not a tautology.

  (c) Show that the implication \( (p \land q) \to (p \lor q) \) is a tautology.
First examples of proofs.

(a) If \( n^2 \) is even, then \( n \) is even.

**Proof.** Indeed, assume that \( n \) is odd, i.e., \( n = 2k + 1 \), then \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \) is odd. We showed that the implication
\[
\{ \text{n is odd} \} \rightarrow \{ \text{n^2 is odd} \} \quad (\neg q \rightarrow \neg p)
\]
is true. It is equivalent to the implication
\[
\{ \text{n^2 is even} \} \rightarrow \{ \text{n is even} \} \quad (p \rightarrow q)
\]
which is true as well.

(b) \( \sqrt{2} \) is irrational number. 

**Proof.** Assume that \( \sqrt{2} = \frac{m}{n} \), where \( m, n \in \mathbb{Z}_+ \), \( n \neq 0 \), and \( m, n \) do not have common divisors, i.e., \( \gcd(m, n) = 1 \). Then we have: \( 2n^2 = m^2 \). Thus \( m^2 \) is even, then by (a), \( m \) is even, i.e., \( m = 2k \). We obtain \( 2n^2 = 4k^2 \) or \( n^2 = 2k^2 \), i.e., \( n \) is even as well. We obtain that \( m, n \) do have a common divisor 2. Contradiction. Thus \( \sqrt{2} \) is irrational number.

Let \( n, k \in \mathbb{Z}_+ \). Recall that \( k \) divides \( n \) if \( n = k \cdot i \) for some \( i \in \mathbb{Z}_+ \). We denote \( k|n \) if \( k \) divides \( n \). Then a number \( p \in \mathbb{Z}_+ \) is prime if it has no divisors other than 1 and \( p \). Here is the list of first few prime numbers:

\[
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 83, 89, 97, 101, \ldots
\]
The closest two prime numbers to 2014 are 2011 and 2017.

There is a remarkable property of positive integers: Let \( S \subset \mathbb{Z}_+ \) be a non-empty subset. Then \( S \) has a minimal element, i.e. such \( n_0 \in S \) that \( n_0 \leq n \) for any \( n \in S \). We will return this later on, this property is called Well Ordering Principle, see Chapter 3 of the textbook.

(c) Let \( n \in \mathbb{Z}_+ \). Then \( n \) is either a prime number or there exists a prime \( p \) such that \( p \) divides \( n \).

**Proof.** Assume there are integers \( n \) which are not primes and no prime \( p \) divides \( n \). Let \( S \) be a set of such integers, and \( n_0 \in S \) is a minimal number. Since \( n_0 \) is not a prime, there exists \( n_1 < n_0 \) with divides \( n_0 \). Since \( n_1 < n_0 \), \( n_1 \) is either prime or it is divisible by a prime. We arrive to a contradiction in both cases.

(d) Now we can follow Euclid (who notice that more than 2500 years ago) to prove the following

**Theorem.** There is infinite number of primes.

**Proof.** Assume there exist only finite number of primes. Let \( P = \{p_1, p_2, \ldots, p_k\} \) is the set of all prime numbers, \( |P| = k \). Consider the integer: \( p_{k+1} = p_1 \cdot p_2 \cdots p_k + 1 \). The integer \( p_{k+1} \) is either pime or not. If \( p_{k+1} \) is not a prime, then it has to be divisible by some prime \( p_j, j = 1, \ldots, k \), but it is not since the remainder will be 1. Thus \( p_{k+1} \) is a prime, and \( p_{k+1} \in P \). Then \( |P| = k + 1 \), not \( |P| = k \). This two properties cannot hold together. Contradiction.

- **Contradiction and other rules of inference.** Above we followed the same scheam: we assume that a statement \( p \) is wrong, or \( \neg p \) is correct, and then we derived a contradiction. This is justified by the tautology \( \neg p \rightarrow \text{F}_0 \rightarrow p \). This can be written as 

\[
\frac{\neg p \rightarrow \text{F}_0}{\therefore p}
\]

Here \( \neg p \rightarrow \text{F}_0 \) is a premise, and \( p \) is a conclusion. The sign “\( \therefore \)” means therefore, and the formula above reads “\( \neg p \rightarrow \text{F}_0 \) is true, therefore, \( p \) true.”
There are several standard rules of inference:

(1) \[ \begin{align*}
   p &
   \quad \rightarrow \quad q \\
   \therefore &\quad p
\end{align*} \]
   Modus Ponens or Rule of Detachment

(2) \[ \begin{align*}
   p &
   \quad \rightarrow \quad q \\
   q &
   \quad \rightarrow \quad r \\
   \therefore &\quad r
\end{align*} \]
   Law of Syllogism

(2) \[ \begin{align*}
   p &
   \quad \rightarrow \quad q \\
   \neg &\quad q \\
   \therefore &\quad \neg p
\end{align*} \]
   Modus Tollens

(3) \[ \begin{align*}
   p &
   \quad \rightarrow \quad q \\
   \therefore &\quad p \land q
\end{align*} \]
   Rule of Conjunction

(4) \[ \begin{align*}
   p &
   \quad \lor \quad q \\
   \neg &\quad q \\
   \therefore &\quad p
\end{align*} \]
   Rule of Disjunctive Syllogism

(5) \[ \begin{align*}
   \neg p &
   \quad \rightarrow \quad F_0 \\
   \therefore &\quad p
\end{align*} \]
   Rule of Contradiction

(6) \[ \begin{align*}
   p &
   \quad \land \quad q \\
   \therefore &\quad p
\end{align*} \]
   Rule of Disjunctive Amplification

(7) \[ \begin{align*}
   p &
   \therefore &\quad p \lor q
\end{align*} \]
   Rule of Conjunctive Simplification

(8) \[ \begin{align*}
   p &
   \quad \rightarrow \quad (q \quad \rightarrow \quad r) \\
   \therefore &\quad r
\end{align*} \]
   Rule of Conditional Proof

(9) \[ \begin{align*}
   p &
   \quad \rightarrow \quad r \\
   q &
   \quad \rightarrow \quad r \\
   \therefore &\quad (p \lor q) \quad \rightarrow \quad r
\end{align*} \]
   Rule of Proof by Cases

(10) \[ \begin{align*}
   p &
   \quad \lor \quad r \\
   \therefore &\quad q \lor s
\end{align*} \]
   Constructive Dilemma

(11) \[ \begin{align*}
   p &
   \quad \lor \quad r \\
   \therefore &\quad \neg q \lor \neg r
\end{align*} \]
   Destructive Dilemma