Summary on Lecture 7, February 6, 2019

- **Sets and subsets.** Usually we work with a given "universe" $\mathcal{U}$ which contains all our sets.
  First examples:

  (1) $\{ \ n \in \mathbf{Z}_+ \mid n^2 = 9 \ \} = \{3\}$;
  (2) $\{ \ n \in \mathbf{Z} \mid n^2 = 9 \ \} = \{-3, 3\}$;
  (3) $\{ \ n \in \mathbf{Z} \mid n^2 = 7 \ \} = \emptyset$;
  (4) $\{ \ n \in \mathbf{R} \mid n^2 = 7 \ \} = \{-\sqrt{7}, \sqrt{7}\}$.

  Definition. Let A, B be two sets. Then $A \subseteq B$ iff $\forall x[(x \in A) \to (x \in B)]$ is a tautology. Then we say that A is a subset of B. Next, the sets A, B are equal iff $A \subseteq B$ and $B \subseteq A$. Then we write $A \subset B$ iff $A \subseteq B$ and $A \neq B$. If $A \subset B$, we say that A is *proper* subset of B.

  Here are short ways to define:

$$\begin{array}{rcl} A \subset B & \iff & [(A \subseteq B) \wedge (A \neq B)] \\ A = B & \iff & [(A \subseteq B) \wedge (B \subseteq A)] \end{array}$$

  Theorem 1. Let $A, B, C \subset \mathcal{U}$. Then

  (a) $A \subseteq B$, $B \subseteq C \implies A \subseteq C$;
  (b) $A \subset B$, $B \subseteq C \implies A \subset C$;
  (c) $A \subseteq B$, $B \subset C \implies A \subset C$;
  (d) $A \subset B$, $B \subset C \implies A \subset C$.

  We give a proof of (b) assuming (a). We already know that $A \subseteq C$. We should show that $A \neq C$. By assumption, $A \subset B$, thus there exists $x \in B$, such that $x \notin A$. Since $B \subseteq C$, $x \in C$. We found an element $x \in C$ such that $x \notin A$, i.e., $A \subset C$.

  Special sets: $\emptyset$, $\mathcal{U}$. By definition, an empty set, denoted by $\emptyset$, is a set with no elements. In particular, $\emptyset \subset A$ for any set A.

  Theorem 2. Let $A \subset \mathcal{U}$. Then $\emptyset \subseteq A$. If $A \neq \emptyset$, then $\emptyset \subset A$.

  Give a proof of Theorem 2.

  Again, let $A \subset \mathcal{U}$. We consider the set of all subsets of A:

$$\mathcal{P}(A) = \{ \ B \mid B \subseteq A \ \}.$$

  Assume that A is a finite set, $A = \{a_1, \ldots, a_n\}$, i.e. $|A| = n$.

  Lemma. Assume $|A| = n$. Then $|\mathcal{P}(A)| = 2^n$.

  Proof. Let $\Sigma = \{0, 1\}$ be the binary alphabet. Consider the set of words Σ^n, i.e., all binary words of length n. We notice that every word in Σ^n corresponds to a subset in A. Place all elements of A next to a binary sequence:

$$\begin{array}{ccccccccc} a_1 & a_2 & a_3 & \cdots & a_{k-1} & a_k & a_{k+1} & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 1 \end{array}$$

  Then all 1's in binary sequence mark the elements to choose for a subset B. Clearly any subset B gives a corresponding binary sequence as well. Thus $|\mathcal{P}(A)| = |\Sigma^n| = 2^n$. $\square$

For the same A, let $k \leq n = |A|$, we define

$$\mathcal{P}_k(A) = \{ \ B \mid (B \subseteq A) \wedge (|B| = k) \ \}.$$

Then it is easy to see that $|\mathcal{P}_k(A)| = \begin{pmatrix} n \\ k \end{pmatrix}$. Summing up, we obtain the formula:

$$\sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} = 2^n$$

We prove again the Pascal's formula.

Lemma. Let $k \leq n+1$. Then $\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix}$.

Proof. Let $A = \{a_1, \ldots, a_n, z\}$. Consider the set $\mathcal{P}_k(A)$. It splits into two subsets: $\mathcal{P}_k(A) = \mathcal{P}_k(A)_z \cup \mathcal{P}_k(A)_{\neg z}$, where $\mathcal{P}_k(A)_z$ contains all subset $B \subset A$ which contain the element z, and $\mathcal{P}_k(A)_{\neg z}$ contains all subset $B \subset A$ which do contain the element z. Clearly, $|\mathcal{P}_k(A)_z| = \begin{pmatrix} n \\ k-1 \end{pmatrix}$ since for $B \in \mathcal{P}_k(A)_z$, it is enough to choose all elements but z. Then $|\mathcal{P}_k(A)_{\neg z}| = \begin{pmatrix} n \\ k \end{pmatrix}$ since for $B \in \mathcal{P}_k(A)_z$, it is enough to choose all elements from the set $\{a_1, \ldots, a_n\}$. Also, it is clear that the sets $\mathcal{P}_k(A)_z$ and $\mathcal{P}_r(A)_{\neg z}$ do not intsersect. $\square$

We define $A \cup B$, $A \cap B$ and $\bar{A}$:

$$\begin{array}{l} (x \in A \cup B) \Longleftrightarrow (x \in A) \vee (x \in B) \\ (x \in A \cap B) \Longleftrightarrow (x \in A) \wedge (x \in B) \\ (x \in \bar{A}) \Longleftrightarrow (x \notin A) \end{array}$$

We say that A and B are *disjoint* if $A \cap B = \emptyset$.

Theorem 3. Let $A, B \subset \mathcal{U}$. The following statements are equivalent:

(a) $A \subseteq B$

(b) $A \cup B = B$

(c) $A \cap B = A$

(b) $\bar{B} \subseteq \bar{A}$

Exercise. Prove Theorem 3.

The following identities to prove:

(1) $\overline{\overline{A}} = A$

(2) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$

(3) $A \cup B = B \cup A$
$A \cap B = B \cap A$

(4) $A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$

(5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(6) $A \cup A = A$
$A \cap A = A$

(7) $A \cup \emptyset = A$
$A \cap \mathcal{U} = A$

(8) $A \cup \overline{A} = \mathcal{U}$
$A \cap \overline{A} = \emptyset$

(9) $A \cup \mathcal{U} = \mathcal{U}$
$A \cap \emptyset = \emptyset$

(10) $A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$

Exercise. Prove (5) and (10) above.

- **Counting again.** Let A_1, A_2 be finite sets. We recall that $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Now we would like to understand the case of three sets:

$$\begin{aligned} |A_1 \cup (A_2 \cup A_3)| &= |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)| \\ &= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| - |A_1 \cap (A_2 \cup A_3)| \end{aligned}$$

We notice:

$$A_1 \cap (A_2 \cup A_3) = (A_1 \cap A_2) \cup (A_1 \cap A_3),$$

where we see:

$$\begin{aligned} |A_1 \cap (A_2 \cup A_3)| &= |A_1 \cap A_2| + |A_1 \cap A_3| - |(A_1 \cap A_2) \cap (A_1 \cap A_3)| \\ &= |A_1 \cap A_2| + |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

We obtain the formula:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Question: What would be a general formula for $A_1, \ldots, A_n$?

- **Well-Ordering Principle.** We recall the Well-Ordering Principle:

If $A \subset \mathbf{Z}_+$, and $A \neq \emptyset$, then there exists a smallest element in A.

- **Mathematical Induction.** Let $S(n)$ be an open proposition, where $n \in \mathbf{Z}_+$.

Theorem 4. Assume that
(B) $S(1)$ is a true statement
(I) $S(k) \to S(k+1)$ is true for all k.

Then $S(n)$ vis a true statement for each n.

Proof. Assume Theorem 4 is false. Then there exists an open statement $S(n)$ which satisfies (B) and (I), however, there exists $m \in \mathbf{Z}_+$ such that $S(m)$ is false. We consider the set:

$$A = \{\ m \in \mathbf{Z}_+ \mid S(m) \text{ is false }\}$$

By the assumption, $A \neq \emptyset$. Then there exists a smallest element n_0 in A, i.e., $S(n_0)$ false, and $S(n)$ is true for all $n < n_0$. We notice that $n_0 > 1$ since $S(1)$ is true. Then we see that $S(n_0 - 1)$ is true statement. Then the implication $S(n_0 - 1) \to S(n_0)$ is true statement; thus $S(n_0)$ is true. Contradiction.

Exercises:

(1) Prove that $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$;

(2) Prove that $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$;

(3) Prove that $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$;

(4) Prove that $8^n - 2^n$ is divisible by 6 for every $n \in \mathbf{Z}_+$.

(5) Prove that $11^n - 4^n$ is divisible by 7 for every $n \in \mathbf{Z}_+$.

(6) Prove that $8^{n+2} + 9^{2n+1}$ is divisible by 73 for every $n \in \mathbf{Z}_+$.