1. **Definition.**

   Let K, L be sets. We say K is a **subset** *of L if the statement (†) holds:*

   (†) *For any object x, [if ($x \in K$) then ($x \in L$)].*

   We write $K \subset L$.

   Definition.

   Let A be a set. The **power set** *of the set A is defined to be the set $\{S \mid S \text{ is a subset of } A\}$. It is denoted by $\mathfrak{P}(A)$.*

   Remark. By definition, $S \in \mathfrak{P}(A)$ iff $S \subset A$.

2. Refer to the Handout *Examples of proofs for properties of basic set operations*. Recall a few results that we have proved:

   (a) **Statement (3) of Theorem (I).**
   Let K, L, M be sets. Suppose K is a subset of L and L is a subset of M. Then K is a subset of M.

   (b) **Statement (1) of Theorem (IV).**
   Let K, L, M be sets. Suppose K is a subset of L and K is a subset of M. Then K is a subset of $L \cap M$.

   (c) **Statement (3) of Theorem (IV).**
   Let K, L, M be sets. Suppose K is a subset of M and L is a subset of M. Then $K \cup L$ is a subset of M.

   We shall take these results for granted in the argument for Theorem ($\dagger_1$).

3. **Theorem ($\dagger_1$).**

   Let A, B be sets. The statements below hold:

   1. $\emptyset, A \in \mathfrak{P}(A)$. *Moreover,* $\mathfrak{P}(A) \neq \emptyset$.
   2. (a) *Suppose* $A \subset B$. *Then* $\mathfrak{P}(A) \subset \mathfrak{P}(B)$.
      (b) *Suppose* $\mathfrak{P}(A) \subset \mathfrak{P}(B)$. *Then* $A \subset B$.
      (c) $A \subset B$ *iff* $\mathfrak{P}(A) \subset \mathfrak{P}(B)$.
   3. $\mathfrak{P}(A \cap B) = \mathfrak{P}(A) \cap \mathfrak{P}(B)$.
   4. $\mathfrak{P}(A) \cup \mathfrak{P}(B) \subset \mathfrak{P}(A \cup B)$.

   Proof of Theorem ($\dagger_1$). Let A, B be sets.

   1. $\emptyset, A$ are subsets of A. Then, by definition, $\emptyset, A \in \mathfrak{P}(A)$.
      Since $\emptyset \in \mathfrak{P}(A)$, we have $\mathfrak{P}(A) \neq \emptyset$.
   2. (a) Suppose $A \subset B$.
         - Pick any $S \in \mathfrak{P}(A)$. By definition, $S \subset A$.
           Since $S \subset A$ and $A \subset B$, we have $S \subset B$. Then by definition, $S \in \mathfrak{P}(B)$.

         It follows that $\mathfrak{P}(A) \subset \mathfrak{P}(B)$.
      (b) Suppose $\mathfrak{P}(A) \subset \mathfrak{P}(B)$.
         Note that $A \in \mathfrak{P}(A)$.
         Since $A \in \mathfrak{P}(A)$ and $\mathfrak{P}(A) \subset \mathfrak{P}(B)$, we have $A \in \mathfrak{P}(B)$. Then, by definition, $A \subset B$.
      (c) It follows from (2a), (2b) that $A \subset B$ iff $\mathfrak{P}(A) \subset \mathfrak{P}(B)$.
   3. - Since $A \cap B \subset A$, we have $\mathfrak{P}(A \cap B) \subset \mathfrak{P}(A)$ by (2a).
        Since $A \cap B \subset B$, we have $\mathfrak{P}(A \cap B) \subset \mathfrak{P}(B)$ by (2a).
        Then $\mathfrak{P}(A \cap B) \subset \mathfrak{P}(A) \cap \mathfrak{P}(B)$. (Why?)
      - Pick any $S \in \mathfrak{P}(A) \cap \mathfrak{P}(B)$.
        Then $S \in \mathfrak{P}(A)$ and $S \in \mathfrak{P}(B)$.
        Since $S \in \mathfrak{P}(A)$, we have $S \subset A$. Since $S \in \mathfrak{P}(B)$, we have $S \subset B$.
        Now $S \subset A$ and $S \subset B$. Then $S \subset A \cap B$. (Why?) Therefore, by definition, $S \in \mathfrak{P}(A \cap B)$.

      It follows that $\mathfrak{P}(A \cap B) = \mathfrak{P}(A) \cap \mathfrak{P}(B)$.

4. Since $A \subset A \cup B$, we have $\mathfrak{P}(A) \subset \mathfrak{P}(A \cup B)$ by (2a).
   Since $B \subset A \cup B$, we have $\mathfrak{P}(B) \subset \mathfrak{P}(A \cup B)$ by (2a).
   Therefore $\mathfrak{P}(A) \cup \mathfrak{P}(B) \subset \mathfrak{P}(A \cup B)$. (Why?)

4. When Statement (3) and Statement (4) of Theorem ($\dagger_1$) are put side-by-side together, it is natural for us to ask whether Statement ($\ddagger$) below is true:

   ($\ddagger$) *Let A, B be sets. $\mathfrak{P}(A \cup B) = \mathfrak{P}(A) \cup \mathfrak{P}(B)$.*

   In light of the validity of Statement (4) of Theorem ($\dagger_1$), Statement ($\ddagger$) is true iff Statement ($\ddagger'$) below is true:

   ($\ddagger'$) *Let A, B be sets. $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$.*

   At this moment, we do not know whether ($\ddagger'$) is true or not. (So there is no point in hurry to give a proof for Statement ($\ddagger'$).) A useful approach to find the answer is to ask Question ($\diamondsuit$):

   ($\diamondsuit$) What happens to the sets A, B if the conclusion '$\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$' holds?

   Answer for Question ($\diamondsuit$):

   - Suppose $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$ indeed.
     Then, as $A \cup B \in \mathfrak{P}(A \cup B)$, we have $A \cup B \in \mathfrak{P}(A) \cup \mathfrak{P}(B)$.
     Therefore $A \cup B \in \mathfrak{P}(A)$ or $A \cup B \in \mathfrak{P}(B)$.
     - (Case 1). Suppose $A \cup B \in \mathfrak{P}(A)$. Then $A \cup B \subset A$. Therefore, since $B \subset A \cup B$, we have $B \subset A$.
     - (Case 2). Suppose $A \cup B \in \mathfrak{P}(B)$. Then modifying the argument above, we obtain $A \subset B$.

     Hence $A \subset B$ or $B \subset A$. (Why?)

   This exploration suggests that we should not expect ($\dagger'$) to be a true statement: it is non-trivial for the sets A, B to satisfy the condition '($A \subset B$ or $B \subset A$)'.

5. In fact a necessary condition for

   $$\text{`}\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)\text{'}$$

   is given by

   $$\text{`}(A \subset B \text{ or } \subset A)\text{'}.$$

   (This is the mathematical content of Statement (1) of Theorem ($\dagger_2$) below. Its proof is constituted by the mathematical argument done in the exploration above.)

   It also turns out that this necessary condition is sufficient as well. (This is the mathematical content of Statement (2) of Theorem ($\dagger_2$). The proof is left as an exercise.)

   Theorem ($\dagger_2$).
   Let A, B be sets. The statements below hold:

   1. *Suppose $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$. Then ($A \subset B$ or $B \subset A$).*
   2. *Suppose ($A \subset B$ or $B \subset A$). Then $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$.*
   3. *$\mathfrak{P}(A \cup B) = \mathfrak{P}(A) \cup \mathfrak{P}(B)$ iff ($A \subset B$ or $B \subset A$).*

6. **Theorem ($\star$). (Basic results in set language from another viewpoint.)**

Let M be a set.

1. *$\mathfrak{P}(M)$ is partially ordered by the subset relation in the sense that the statements below hold:*
   (a) *$A \subset A$ for any $A \in \mathfrak{P}(M)$.*
   (b) *For any $A, B \in \mathfrak{P}(M)$, if $A \subset B$ and $B \subset A$ then $A = B$.*
   (c) *For any $A, B, C \in \mathfrak{P}(M)$, if $A \subset B$ and $B \subset C$ then $A \subset C$.*
2. *$\mathfrak{P}(M)$ together with the set operations intersection, union, and complement in M constitutes a boolean algebra in the sense that the statements below hold:*
   (a) *$A \cap B = B \cap A$ for any $A, B \in \mathfrak{P}(M)$.*
   (a') *$A \cup B = B \cup A$ for any $A, B \in \mathfrak{P}(M)$.*
   (b) *$(A \cap B) \cap C = A \cap (B \cap C)$ for any $A, B, C \in \mathfrak{P}(M)$.*
   (b') *$(A \cup B) \cup C = A \cup (B \cup C)$ for any $A, B, C \in \mathfrak{P}(M)$.*
   (c) *$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ for any $A, B, C \in \mathfrak{P}(M)$.*
   (c') *$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ for any $A, B, C \in \mathfrak{P}(M)$.*
   (d) *$A \cap \emptyset = \emptyset$ for any $A \in \mathfrak{P}(M)$. ($\emptyset$ is a unity for $\cap$ in $\mathfrak{P}(M)$.)*
   (d') *$A \cup M = M$ for any $A \in \mathfrak{P}(M)$. (M is a unity for $\cup$ in $\mathfrak{P}(M)$.)*
   (e) *$A \cap (M \backslash A) = \emptyset$ for any $A \in \mathfrak{P}(M)$. ($M \backslash A$ is an inverse of A with respect to $\cap$.)*
   (e') *$A \cup (M \backslash A) = M$ for any $A \in \mathfrak{P}(M)$. ($M \backslash A$ is an inverse of A with respect to $\cup$.)*
   (f) *$A \cap (A \cup B) = A$ for any $A, B \in \mathfrak{P}(M)$.*
   (f') *$A \cup (A \cap B) = A$ for any $A, B \in \mathfrak{P}(M)$.*
   (g) *$M \backslash (A \cap B) = (M \backslash A) \cup (M \backslash B)$ for any $A \in \mathfrak{P}(M)$.*
   (g') *$M \backslash (A \cup B) = (M \backslash A) \cap (M \backslash B)$ for any $A \in \mathfrak{P}(M)$.*
   (h) *$M \backslash (M \backslash A) = A$ for any $A \in \mathfrak{P}(M)$.*
3. *$\mathfrak{P}(M)$ forms an abelian group with symmetric difference in M as group operation in the sense that the statements below hold:*
   (a) *$A \triangle B \in \mathfrak{P}(M)$ for any $A, B \in \mathfrak{P}(M)$.*
   (b) *$A \triangle B = B \triangle A$ for any $A, B \in \mathfrak{P}(M)$.*
   (c) *$(A \triangle B) \triangle C = A \triangle (B \triangle C)$ for any $A, B, C \in \mathfrak{P}(M)$.*
   (d) *$A \triangle \emptyset = A = \emptyset \triangle A$ for any $A \in \mathfrak{P}(M)$. ($\emptyset$ is an identity element of $\mathfrak{P}(M)$ with respect to $\triangle$.)*
   (e) *$A \triangle A = \emptyset$ for any $A \in \mathfrak{P}(A)$. (A is an inverse element of $\mathfrak{P}(M)$ with respect to $\triangle$.)*

Remarks on terminologies.

- (1a), (1b), (1c) are respectively known as the Law of Reflexivity, the Law of Anti-symmetry, the Law of Transitivity.
- (2a), (2a') are known as the Laws of Commutativity. (2b), (2b') are known as the Laws of Associativity. (2c), (2c') are known as the Distributive Laws. (2d), (2d') are known as the Laws of Existence of Unity. (2e), (2e') are known as the Laws of Existence of Inverse. (2f), (2f') are known as the Laws of Absorption. (2g), (2g') are known as De Morgan's Laws. (2h) are known as the Law of Double Negation.
- (3a), (3b), (3c), (3d), (3e) are collectively referred to as the axioms of abelian groups.