Lesson 1: Preliminaries

Theme: Some useful notations and facts from discrete mathematics.

1 Sets

- A set is a collection of things, which are called its members or elements.\n  \( a \in X \) (read: \( a \) is in \( X \), or \( a \) belongs to \( X \)) means \( a \) is a member or an element of \( X \). \( a \notin X \) means that \( a \) is not a member of \( X \).
- An empty set is denoted by \( \emptyset \).
- \( X \) is a subset of \( Y \), denoted by \( X \subseteq Y \), if every element of \( X \) is also an element of \( Y \).
- \( X \) is a proper subset of \( Y \), denoted by \( X \subset Y \), if \( X \neq Y \) and \( X \subseteq Y \).
- For two sets \( X \) and \( Y \), we write \( X \cap Y \) and \( X \cup Y \) to denote their intersection and union, respectively.
- Let \( X \) be a set whose elements are also sets. Then, \( \bigcup X \) and \( \bigcap X \) denote the following.
  \[
  \bigcup X := \{ a \mid a \text{ belongs to an element in } X \}
  \]
  \[
  \bigcap X := \{ a \mid a \text{ belongs to every element in } X \}
  \]
- The cartesian product between two sets \( X \) and \( Y \) is the following.
  \[
  X \times Y := \{ (a, b) \mid a \in X \text{ and } b \in Y \}.
  \]
  We write \( X^n \) to denote \( X \times \cdots \times X \) (\( X \) appears \( n \) times).

2 Relations

- A relation \( R \) over two sets \( X, Y \) is a subset of \( X \times Y \).
- A binary relation \( R \) over \( X \) is a subset of \( X \times X \).
- An \( n \)-ary relation \( R \) over \( X \) is a subset of \( X^n \).

3 Functions

- A relation \( R \) over \( X, Y \) is a function or a mapping, if for every \( x \in X \), there is exactly one \( y \in Y \) such that \( (x, y) \in R \).
  In this case, we will say \( R \) is a function from \( X \) to \( Y \), or \( R \) maps \( X \) to \( Y \). We denote it by \( R : X \to Y \).
- We will usually use the letters \( f, g, h, \ldots \) to represent functions. As usual, we write \( f(x) \) to denote the element \( y \) in which \( (x, y) \in f \).
- A function \( f : X \to Y \) is an injective function, if for every \( y \in Y \), there is at most one \( x \in X \) such that \( f(x) = y \). An injective functions is also called an injection.
- A function \( f : X \to Y \) is a surjective function, if for every \( y \in Y \), there is at least one \( x \in X \) such that \( f(x) = y \).
- A function \( f : X \to Y \) is a bijection, if it is both injective and surjective.
4 Equivalence relations

A binary relation $R$ over $X$ is called an equivalence relation, if it satisfies the following conditions.

- Reflexive: $(x, x) \in R$, for every $x \in X$.
- Symmetric: $(x, y) \in R$ if and only if $(y, x)$, for every $x, y \in X$.
- Transitive: for every $x, y, z \in X$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

For $x \in X$, the equivalence class of $x$ in $R$ is defined as:

$$[x]_R := \{ y \mid (x, y) \in R \}$$

**Lemma 1.1** Let $R$ be an equivalence relation over $X$. Then, the following holds:

- $[x]_R = [y]_R$ if and only if $(x, y) \in R$.
- If $[x]_R \neq [y]_R$, then $[x]_R \cap [y]_R = \emptyset$.

**Theorem 1.2** Let $R$ be an equivalence relation over $X$. Then, the equivalence classes of $R$ partition $X$, i.e., every member of $X$ belongs to exactly one equivalence class of $R$.

5 Countable and uncountable sets

Let $\mathbb{N}$ be the set of natural numbers $\{0, 1, 2, \ldots \}$. A set $X$ is countable, if there is an injective function from $X$ to $\mathbb{N}$. Otherwise, it is called an uncountable set.

**Theorem 1.3** The following sets are all countable.

1. The set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots \}$ of integers.
2. The set $\mathbb{N}^k$, for every integer $k \geq 1$.
3. The set $\mathbb{N}^* := \bigcup_{k \geq 1} \mathbb{N}^k$.

**Theorem 1.4** The set $\mathcal{P}^\mathbb{N}$ is uncountable.

6 Poset (partially ordered set)

Let $X$ be a set and $R$ be a binary relation on $X$. The set $X$ is a poset (w.r.t. $R$), if $R$ is reflexive, anti-symmetric and transitive.

**Definition 1.5** An element $m \in X$ is a maximal element in a poset $X$ (w.r.t. $R$), if for every $x \in X$ and $x \neq m$, $(m, x) \notin R$.

**Definition 1.6** A subset $C$ of $X$ is a chain in $X$ (w.r.t. $R$), if for every $x, y \in C$, either $(x, y) \in R$, or $(y, x) \in R$. A chain $C$ is bounded, if there is $z \in X$ such that for every $x \in C$, $(x, z) \in R$.

---

*A binary relation $R$ on $X$ is anti-symmetric, if the following holds: for every $a, b \in X$, if both $(a, b)$ and $(b, a)$ are in $R$, then $a = b$. 

---
Exercises

(1) Let $A$ and $B$ be sets.

Prove that $x \not\in A \cup B$ if and only if $x \not\in A$ and $x \not\in B$, and in particular, $\overline{A \cup B} = \overline{A} \cap \overline{B}$, where $\overline{X}$ denotes the complement of $X$, i.e., the set of elements not in $X$.

Likewise, prove that $x \not\in A \cap B$ if and only if $x \not\in A$ or $x \not\in B$, and in particular, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

(2) Prove Lemma 1.1 and Theorem 1.2.

(3) Prove Theorem 1.3 in the lecture note.

(4) Prove Theorem 1.4 in the lecture note.

(5) Let $\mathbb{R}$ be the set of real numbers. Define a relation $R$, where $(x, y) \in R$ if and only if $x < y$.

Prove that $\mathbb{R}$ is a poset w.r.t. $R$.

(6) Give an example of a bounded chain in the poset $(\mathbb{R}, \leq)$ as defined in question 4.

(7) Give an example of an unbounded chain in the poset $(\mathbb{R}, \leq)$.

(8) Let $A$ be a set and $\mathcal{F}$ be a collection of subsets of $A$. Define a relation $R$ on elements of $\mathcal{F}$:

$$(x, y) \in R \text{ if and only if } x \subseteq y$$

Prove that $\mathcal{F}$ is a poset w.r.t. $R$.

(9) Give an example of a poset $(\mathcal{F}, \subseteq)$ in which every chain is bounded.

(10) Give an example of a poset $(\mathcal{F}, \subseteq)$ in which there is an unbounded chain.

(11) Consider a poset $(\mathcal{F}, \subseteq)$ where $\mathcal{F}$ is a collection of subsets of a set $A$. Suppose that for every chain $C$ in $\mathcal{F}$, the set $\bigcup C$ is in $\mathcal{F}$.

Assuming Zorn’s lemma, prove that there is an element $M \in \mathcal{F}$ such that there is no $X \in \mathcal{F}$ where $M \subsetneq X$.

---

†The poset $\mathbb{R}$ w.r.t. the relation $\leq$ is usually written as $(\mathbb{R}, \leq)$.

‡The poset $\mathcal{F}$ w.r.t. the relation $\subseteq$ is usually written as $(\mathcal{F}, \subseteq)$. 
Appendix

The three statements below are equivalent and they are usually taken as “axioms” in mathematics.

**Axiom of choice:** Let $I$ be a set such that each $i \in I$ is associated with a set $A_i$. There is a function $f : I \to \bigcup A_i$ such that for every $i \in I$, $f(i) \in A_i$.

**Zorn’s lemma:** Let $(A, R)$ be a poset such that every chain in $A$ is bounded. There is an element $m \in A$ such that for every $x \in A$ and $x \neq m$, $(m, x) \notin R$.

**Well-ordering theorem:** Every set can be well-ordered. That is, for every set $A$, there is a total order relation $R$ on $A$, that is, it satisfies the following conditions:

- Antisymmetry: for every $a, b \in A$, if $(a, b), (b, a) \in R$, then $a = b$;
- Transitive: if $(a, b), (b, c) \in R$, then $(a, c) \in R$;
- Totality: for every $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$,

such that for every nonempty subset $B \subseteq A$ has a minimal element (w.r.t. $R$).

There is a kind of contradiction here: the axiom of choice is viewed as obviously “correct,” while the well-ordering theorem is obviously “false,” and there are mixed opinions about Zorn’s lemma.