Lecture 1: Preliminaries

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is the **cartesian product** of A and B.

Definition (Relation)

A **relation** between sets A and B is a subset R of $A \times B$.

- If $(a, b) \in R$, then we say that "a is related to b" and denote it as $a\mathbf{R}b$.
- Any relation between a set S to S is called a **relation on** S.

Definition (Equivalence relation)

A relation **R** on a set S is called an **equivalence relation** if the followings are satisfied for all $x, y, z \in S$:

1. **Reflexive:** xRx.
2. **Symmetric:** If xRy, then yRx.
3. **Transitive:** If xRy and yRz, then xRz.

Partitions and Equivalence Relations

A **partition** of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. These subsets are called as the **cells** of the partition.

Theorem

Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition of S where

$$\overline{a} = \{x \in S \mid x \sim a\}.$$

Also each partition of S gives rise to an equivalence relation $\sim$ on S where

$$a \sim b \Leftrightarrow \text{ a and b are in the same cell of partition.}$$

Each cell in the partition arising from an equivalence relation is an equivalence class.

Functions

If every element of A is related to exactly one element of B, then we have the relation, called as **function.**

Definition

Let A and B be nonempty sets. f is called a **function** from A to B, denoted $f : A \longrightarrow B$, if f is a relation from A to B with the property that every element a in A is the first coordinate of exactly one ordered pair in f. That is,

1. For each element $a \in A$, there is an element $b \in B$ such that $(a, b) \in f$. ($\forall a \in A, \exists b \in B$ such that $f(a) = b$)
2. If $(a, b), (a, c) \in f$, then $b = c$.
   (If $f(a) = b$ and $f(a) = c \Rightarrow b = c$)

Example: Let $A = \{1, 2, 3\}, B = \{a, b, c, d\}$.
$f = \{(1, b), (2, d), (3, b)\}$ is a function
$g = \{(1, a), (\mathbf{2}, c), (3, b), (\mathbf{2}, a)\}$ is not a function.

Functions

Let $f : A \to B$ be a function

- A is called the **domain** of f and B is called the **codomain** of f.
- The **range** of f is $f(A) = \{f(a) \mid a \in A\}$.
- f is called **onto** if $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$.
  $f : A \overset{onto}{\to} B \Leftrightarrow f(A) = B$
- $f : A \overset{1-1}{\to} B$ if $f(a) = f(b)$ implies $a = b$ for all $a, b \in A$.

Let $f : A \to B$ be a function and $D \subseteq A$, $E \subseteq B$.

- $f(D) = \{f(a) \mid a \in D\} \subseteq B$ is called the **range** of f under D.
- $f^{-1}(D) = \{a \mid f(a) \in E\} \subseteq A$ is called the **inverse image** (preimage) of f under E.
  The set $f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\} \subseteq A$

Functions

For a relation $R : A \longrightarrow B$, the inverse relation $R^{-1} : B \longrightarrow A$ is defined by

$$R^{-1} = \{(b, a) \mid (a, b) \in R\} .$$

Every function $f : A \longrightarrow B$ is also a relation from A to B , and so there is an inverse relation f^{-1} from B to A.

We need the following conditions for the inverse relation f^{-1} to be a function.

1. $\forall b \in B, \exists a \in A$ such that $(b, a) \in f^{-1}$. (This implies f must be onto)
2. If $(b, a), (b, c) \in f^{-1}$, then $a = c$. (This implies f must be 1-1)

Thus if $f : A \longrightarrow B$ be a 1-1 and onto function, then $f^{-1} : B \longrightarrow A$ is referred to as the **inverse function** of f.

Remarks:

1. Let A and B be **finite** nonempty sets.

- $f : A \overset{1-1}{\longrightarrow} B \Rightarrow |A| \leq |B|$
- $f : A \overset{onto}{\longrightarrow} B \Rightarrow |A| \geq |B|$
- $f : A \overset{1-1, onto}{\longrightarrow} B \Rightarrow |A| = |B|$

2. Let A and B be **finite** nonempty sets and $|A| = |B|$. Then

$$f \text{ is } 1-1 \Leftrightarrow f \text{ is } \textit{onto}.$$

Binary Operations

Definition

A **binary operation** $*$ on a set S is a function from $S \times S$ to S.

$$* : \quad \begin{array}{ccc} S \times S & \longrightarrow & S \\ (a,b) & \longrightarrow & a*b \end{array}$$

For each $(a, b) \in S \times S$, we denote the element $*((a, b))$ of S by $a * b$.

- Let $*$ be a binary operation on S and let $H \subseteq S$. Then the subset H is **closed under** $*$ if $a * b$ for all $a, b \in H$.

Definition

Let denote $(S, *)$consists of a nonempty set S and a binary operation $*$ on S. We refer to $(S, *)$ as an **algebraic structure.**

Properties of an algebraic structure $(S, *)$:

1. Associative: $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.
2. Identity element: $\exists e \in S$ such that $a * e = e * a = a$ for all $a \in S$.
3. Inverse element: For each $a \in S, \exists a' \in S$ such that $a * a' = a' * a = e$.
4. Commutative: $a * b = b * a$ for all $a, b \in S$.

Congruence Modulo n

Let $n \in \mathbb{Z}^+$ and $x, y \in \mathbb{Z}$. The relation "$\equiv \pmod{n}$" defined by

$$x \equiv y \pmod{n} \Leftrightarrow n \mid x - y$$

is an equivalence relation on $\mathbb{Z}^+$ and called as **congruence modulo** n.
The equivalence classes are called as **residue classes modulo** n (integers modulo n).
For $x \in \mathbb{Z}$,

$$\begin{aligned} \overline{x} &= \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\} \\ &= \{y \in \mathbb{Z} \mid n \mid y - x\} \\ &= \{y \in \mathbb{Z} \mid y - x = nk, \exists k \in \mathbb{Z}\} \\ &= \{x + nk \mid k \in \mathbb{Z}\}. \end{aligned}$$

The set of all congruence classes is denoted by

$$\mathbb{Z}_n := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

and called as the set of residue classes modulo n.

Congruence Modulo n

- The operations $+_n$ and $\cdot_n$ on $\mathbb{Z}_n$ are defined by
$$\begin{aligned} \overline{a} +_n \overline{b} &: = \overline{a+b} \\ \overline{a} \cdot_n \overline{b} &: = \overline{ab} \end{aligned}$$
- $\overline{a} \in \mathbb{Z}_n$ has multiplicative inverse modulo $n \Leftrightarrow \gcd(a, n) = 1$.
- $\mathbb{Z}_n^\star = \{\overline{a} \mid \gcd(a, n) = 1\}$ is called the prime residue classes. $|\mathbb{Z}_n^\star| = \phi(n)$ where ϕ is **Euler-phi function** and defined as the number of positive integers $a \leq n$ such that $\gcd(a, n) = 1$.
  1. $\phi(p) = p - 1$
  2. $\phi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right)$
  3. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\,\phi(n)$
  4. If $m = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, then
  $$\begin{aligned} \phi(m) &= \phi\left(p_1^{r_1}\right) \phi\left(p_2^{r_2}\right) \ldots \phi\left(p_k^{r_k}\right) \\ &= p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$
- $\mathbb{Z}_p^\star = \mathbb{Z}_p - \{\overline{0}\}$, $\left|\mathbb{Z}_p^\star\right| = \phi(p) = p - 1$.