1. $\mathbb{Z}/n\mathbb{Z}$: The integers modulo n

Definition 1.1 (Equivalence relation)**.** Let X and Y be sets. A relation from X to Y is a subset $R \subseteq X \times Y$. If $X = Y$, we say R is a relation on X.

Alternative ways to denote the statament $(x, y) \in R$ are

$$xRy, \qquad x \equiv y \mod R, \qquad x \equiv_R y, \qquad x \sim y.$$

Note the last one is the exactly the same as the first, but the symbol $\sim$ has be chosen instead.

Def: Given sets X and Y, a elation R from X to Y If $X = Y$ we say that n is a elation on X

Definition 1.2. A partition of a set X is a subset $P \subset \mathcal{P}(X)$ such that

(i) $X = \bigcup_{A \in P} A$, and

(ii) if $A, B \in P$, then $A \cap B = \varnothing$

Basically, a partition of a set X is a cover of X by pairwise disjoint sets. Let us present some of the most basic types relations you will encounter in your studies.

Definition 1.3. Let $\sim$ be a relation on a set X. Then

(i) $\sim$ is **reflexive** iff $x \sim x$ for all $x \in X$.

(ii) $\sim$ is **symmetric** iff $x \sim y$ implies $y \sim x$ for all $x, y \in X$.

(iii) $\sim$ is **transitive** iff $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in X$.

(iv) $\sim$ is an **equivalence relation** on X iff $\sim$ is reflexive, symmetric, and transitive.

Exercise 1. Let $X = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$ and

$$\sim \; = \left\{ ((a,b),(c,d)) \in X^2 \mid ad = bc \right\}.$$

Prove $\sim$ is an equivalence relation on X. How does this relates to the equality of two rational numbers?

Definition 1.4. Let $\sim$ be an equivalence relation on a set X. The **equivalence class** of an element $x \in X$ under $\sim$ is the set

$$\{x' \in X \mid x \sim x'\}$$

denoted by $[x]_\sim$ or simply $[x]$ if $\sim$ is understood from the context. An element of $[x]_\sim$ is said to be equivalent to x. If $x' \in [x]_\sim$, we say x' is a representative of $[x]_\sim$.

Any element of a class can be used as a representative of such class. Evidently, $x \in [x]$ for any x. There is nothing special about the particular element chosen as its representative.

Exercise 2. Let $\sim$ be an equivalence relation on a set X.

(i) Prove
$$x \sim y \iff [x] = [y] \iff [x] \cap [y] \neq \varnothing,$$
for any $x, y \in X$.

(ii) Prove
$$\bigcup_{a \in X} [a] = X \quad \text{and} \quad [x] \cap [y] = \varnothing$$
whenever $x \nsim y$.

The last exercise shows that an equivalence relation on a set gives rise to a partition of such a set. The elements of this partition are precisely the equivalence classes induced by the equivalence relation. Conversely, any partition induces an equivalence relation in a natural way. Prove this assertion.

Definition 1.5. Let $\sim$ be an equivalence relation on a set X. The quotient set of X by $\sim$ is the set
$$\{[x] : x \in X\},$$
denoted $X/\sim$.

Example 1. In Exercise 1. we saw the relation $\sim$ on $\mathbb{Z}^2$ defined by
$$(a, b) \sim (c, d) \iff ad = bc$$
is an equivalence relation on $\mathbb{Z}^2$. It turns out $\mathbb{Q} = \mathbb{Z}^2/\sim$. In other words, the rational numbers can be constructed from integers by means of $\sim$.

1.1. Partitioning $\mathbb{Z}$

Let $n \in \mathbb{Z}^+$. The relation on $\mathbb{Z}$ defined by
$$a \sim_n b \iff n \mid (b - a)$$
is an equivalence relation on $\mathbb{Z}$. We write $a \equiv b \bmod n$ whenever $a \sim_n b$. The equivalence class of an integer a under $\sim_n$ is denoted $\bar{a}$ and it is called the congruence class of a mod n.

Definition 1.6. The set of integers modulo n is the set of congruence classes of $\mathbb{Z}$ under $\sim_n$. It is denoted $\mathbb{Z}/n\mathbb{Z}$.

You will see why we have chosen this notation when we discuss ideals in ring theory. There are precisely n congruence classes, namely $[0], [1], \ldots, [n-1]$. Why $[0] = [n]$?

Exercise 3. List all the elements of $\mathbb{Z}/4\mathbb{Z}$.

1.2. Modular operations in $\mathbb{Z}/n\mathbb{Z}$