
Properties of Equivalence Classes

Theorem. Let R be an equivalence relation on a nonempty set A. For $a, b \in A$,

$$[a] = [b] \text{ if and only if } aRb.$$

Theorem. Let R be an equivalence relation on a set $S \neq \emptyset$. For any $x, y \in S$, $[x] = [y]$ if and only if $[x] \cap [y] \neq \emptyset$.

Theorem. Let R be an equivalence relation on a nonempty set A. Then the set

$$P = \{[a] : a \in A\}$$

is a partition of A.

Congruence Modulo m

Definition: Let $m \in \mathbb{N}$. The equivalence classes defined by the congruence relation *modulo* m are called **residue classes modulo** m. For any $a \in \mathbb{Z}$, $[a]$ denotes the equivalence class of a, i.e.

$$[a] = \{b \in \mathbb{Z} \mid a \equiv b \,(mod\, m)\}$$

Theorem (*Congruences as equivalence relation.*) Let $m \in \mathbb{N}$.

The congruence relation modulo m is an equivalence relation on $\mathbb{N}$.

To prove the theorem, check if the following properties for any $a, b \in \mathbb{Z}$ are satisfied.

1. *Reflexivity:* $a \equiv a \,(mod\, m)$
2. *Symmetry:* If $a \equiv b \,(mod\, m)$, then $b \equiv a \;(mod\, m)$
3. *Transitivity:* If $a \equiv b \,(mod\, m)$ and $b \equiv c \,(mod\, m)$, then $a \equiv c \,(mod\, m)$.

Prove that $a \equiv b \pmod 5$ if and only if $9a + b \equiv 0 \pmod 5$ for $a, b \in \mathbb{Z}$.

$\mathbb{Z}_p$: The Integers Modulo p

$\mathbb{Z}_p$ is the set of integers modulo p. In reality the elements of $\mathbb{Z}_p$ are equivalence classes (residue classes),

$$\mathbb{Z}_p = \{[0], [1], ..., [p-1]\}.$$

However, we often write

$$\mathbb{Z}_p = \{0, 1, ..., p-1\}.$$

Consider $\mathbb{Z}_8$. Is it possible to have $a, b \in \mathbb{Z}_8$ with $a \neq 0$ and $b \neq 0$, but $a \cdot b = 0$?

Operations on $\mathbb{Z}_p$

1. Let X be a nonempty set with an operation $\circ$.
   For any $x, y \in X$, if $x \circ y \in X$, then the set X is **closed** under the operation $\circ$.

   Example : $\mathbb{N}$ is closed under the addition "+".

2. Define $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$. Are they **well–defined**?

   $\star$ Draw the addition and multiplication tables for $\mathbb{Z}_4$.

   $\star$ For $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_p$, if $[a + c] = [b + d]$ and $[ac] = [bd]$, then addition and multiplication in $\mathbb{Z}_p$ are well defined.

3. Prove that the addition and multiplication are well defined in $\mathbb{Z}_p$.

4. If we define the "*-product" $[a] * [b] = [q]$ where q is the quotient when ab is divided by 3 for equivalence classes $[a]$ and $[b]$ in $\mathbb{Z}_3$, **disprove** that this *-product is well defined.