Abstract Algebra

Group of residue classes

Definition:- Consider the set Z of integers so that

$$Z = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \cdots\}$$

Let $a, b \in Z$ be arbitrary and n a fixed positive integer.

We define a relation $\equiv (\mathrm{mod}\, n)$ on Z as follows:

$$a \equiv b \ (\mathrm{mod}\, n)$$

iff $a-b$ is divisible by n i.e. iff $a-b = qn$ for some $q \in Z$.

$a \equiv b \ (\mathrm{mod}\, n)$ is read as a is Congruent to b modulo n.

For $-9 \equiv 5 \ (\mathrm{mod}\, 7)$, $2 \equiv 11 \ (\mathrm{mod}\, 3)$

$20 \equiv 2 \ (\mathrm{mod})$ etc.

Theorem:- The set of residue classes modulo m is a group w.r.t. addition of residue classes.

Proof:- Let Z_m denote the set of all residue classes modulo m

so that $Z_m = \{[0], [1], [2], [3], \cdots [m-1]\}$.

Let $[a], [b] \in Z_m$ be arbitrary.

TO prove that $(Z_m, +)$ is a group.

Closure Property..

$$[a], [b] \in Z_m \Rightarrow [a]+[b] \in Z_m.$$

For $[a]+[b] = [r]$, where r is the ~~least~~ least non-negative remainder when $a+b$ is divided by m.

This $\Rightarrow 0 \le r < m \Rightarrow [r] \in Z_m \Rightarrow [a]+[b] \in Z_m$.

Associativity: $([a]+[b])+[c] = [a]+([b]+[c])$

For L.H.S $= ([a]+[b])+[c]$, Where $a+b$ is reduced by m.

$= [(a+b)+c]$, Where $(a+b)+c$ is reduced by m.

$= [a+(b+c)] \quad \because (a+b)+c = a+(b+c)$

$= [a]+[b+c] = [a]+([b]+[c])$

$= R.H.S.$

Existence of Identity element: There exists identity element $[0] \in Z_m$.

For $[0]+[a] = [a] = [a]+[0]$.

Existence of Inverse: Every element $[a] \in Z_m$ has its inverse

$[m-a] \in Z_m$.

For $[a]+[m-a] = [0] = [m-a]+[a]$, Where $a \neq 0$

Thus all the group postulates are Satisfied And hence $(Z_m, +)$ is a group.

Proof

Problem – Do the sets of residue classes module 7 form a group w.r.t. addition?

Solution:– Let Z_7 denote the set of all residue classes module 7, so that $Z_7 = \{[0], [1], [2], [3], [4], --[6]\}$.

To determine the nature of the system $(Z_7, +)$

Putting $m=7$ we get the solution

$O(4) = 7$, Since Z_7 Contains 7 elements.

Finally we have prove that $(Z_7, +)$ is an abelian group of order 7.

Anjani Kumar Singh.

01.06.2021