Addition Modulo m

If a and b are any two integers, and r is the least non-negative reminder obtained by dividing the ordinary sum of a and b by m. then addition modulo m of a & b is r symbolically.

$$a +_m b = r \quad , \quad 0 \leq r < m$$

Ex $\quad 7 +_5 9 = 1$

$$7 + 9 = 16 = 3 \times 5 + 1$$

also $\quad -15 +_5 3 = 2$

$$-15 + 3 = -12 = -5 \cdot 2 - 2$$

In general, if the difference $a - b$ is divisible by m. we can write.

$$a \equiv b \pmod m$$

i.e. "a is congruent to b mod m"

Multiplication modulo p

p is a positive integer of any ~~two~~ two integers a and b is defined as r, where r is the least non-negative remainder when the product of a and b is divided by p. Symbolically we write $a \times_p b = r \quad , \quad 0 \leq r < p$

Ex Show that the set $G = \{0,1,2,3,4\}$ is an abelian Group with respect to addition modulo 5.

Sol^n

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Composition table for elements of G.

The set G is closed under addition modulo 5.

Associativity

For any three element $a, b, c \in G$. Then $(a+b)+c = a+(b+c)$ have a same remainder when it divides by 5

i.e. $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

where $a = 1,\ b = 3,\ c = 4$

$(1 +_5 3) +_5 4 = 4 +_5 4 = 3$

$1 +_5 (3 +_5 4) = 1 +_5 2 = 3$

Existence of identity element

Clearly, $0 \in G$ is the identity element

$0 +_5 4 = 4$

Existence of inverse

0 is its own inverse

4 is the inverse of 1 and 1 is the inverse of 4
2 is the inverse of 3 and 3 is the inverse of 2 w.r.t. addition modulo 5 in G.

Commutative

From this composition table it is clear that

$$a +_5 b = b +_5 a \quad \forall a, b \in G$$

Hence $(G, +_5)$ is an abelian Group.

Elementary properties of Groups

(1) If $(G, *)$ is a group, then identity element in G is unique.

Let e_1, e_2 be identity elements in G.

e_1 is the identity element and $e_2 \in G$.

$$\Rightarrow e_1 * e_2 = e_2 = e_2 * e_1 \quad \text{---} (1)$$

e_2 is the identity element and $e_1 \in G$

$$\Rightarrow e_1 * e_2 = e_1 = e_2 * e_1 \quad \text{---} (2)$$

From eqn (1) & (2), we get

$$\boxed{e_1 = e_2}$$

(2) The inverse of each element in a group $(G, *)$ is unique

Let $a \in G$ and e be the identity element in G

Let $b \in G$ be an inverse of a in G also Let $c \in G$ be an inverse of a in G.

$$a * b = b * a = e \quad [b \text{ is an inverse of } a]$$
$$a * c = c * a = e \quad [c \text{ is an inverse of } a]$$

Now,

$$b = b * e$$
$$b = b * (a * c) \quad [e \text{ is the identity}]$$
$$b = (b * a) * c \quad [\text{associative Law}]$$
$$b = e * c \quad [\text{inverse of } a]$$
$$\boxed{b = c}$$

(3) In a group $(G, *)$

$$(a^{-1})^{-1} = a \quad \forall a \in G.$$

(a^{-1} is an inverse of a)

<u>Proof</u> - G is a group

$\therefore a \in G \Rightarrow a^{-1} \in G$ such that

$$a^{-1} * a = e = a * a^{-1}$$

Now, $a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$ such that

$$(a^{-1}) * (a^{-1})^{-1} = e = (a^{-1})^{-1} * a^{-1}$$

consider $a * a^{-1} = e = a^{-1} * a$

$(a^{-1})^{-1}$ ~~added~~ multiply both sides

$$(a^{-1})^{-1} * [a^{-1} * a] = (a^{-1})^{-1} * e$$

$$((a^{-1})^{-1} * a^{-1}) * a = (a^{-1})^{-1}$$

$$e * a = (a^{-1})^{-1}$$

$$\boxed{a = (a^{-1})^{-1}}$$

$$\therefore (a^{-1})^{-1} = a \quad \forall a \in G$$

(4) If $(G, *)$ is a group $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$

<u>Proof</u>: Let $a, b \in G$ and e be identity element in G.

$a \in G \Rightarrow a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

and $b \in G \Rightarrow b^{-1} \in G$ such that $b^{-1} = b^{-1} * b = e$

<u>Now</u> $a, b \in G \Rightarrow a * b \in G$ and $(ab)^{-1} \in G$.

Consider $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ [associative Law]

$= b^{-1} * e * b$

$= b^{-1} * b$

$= e$

and $(a * b) * (b^{-1} * a^{-1}) = a * (b^{-1} * b^{-1}) * a^{-1}$

$= a * e * a^{-1}$

$= a * a^{-1}$

$= e$

Therefore $(b^{-1} * a^{-1})(a * b) = (a * b)(b^{-1} * a^{-1}) = e$

By Inverse definition $(a * b)^{-1} = b^{-1} * a^{-1}$

(5) Cancellation Law hold good in G i.e. for all $a, b, c \in G$

$a * b = a * c \Rightarrow b = c$ [Left Cancellation Law]

$b * a = c * a \Rightarrow b = c$ [Right Cancellation Law]

Proof: $a \in G \Rightarrow a^{-1} \in G$ such that

$a * a^{-1} = a^{-1} * a = e$, where e is an identity element in G.

Consider $a * b = a * c$

$a^{-1} * (a * b) = a^{-1} * (a * c)$

$(a^{-1} * a) * b = (a^{-1} * a) * c$ (By Associative Law]

$e * b = e * c$ (a^{-1} is the inverse of a]

$\boxed{b = c}$ (e is the identity element]

now, $b * a = c * a$

$(b * a) * a^{-1} = (c * a) * a^{-1}$

$b * (a * a^{-1}) = c * (a * a^{-1})$

$b * e = c * e$

$\boxed{b = c}$

Hence, cancellation Law hold good in G.