Define a relation $\cdot \equiv \cdot \pmod n$ on $\mathbb{Z}$ $\left(\cdot \equiv \pmod n\right)$

as follows;

$a \equiv b \pmod n$ if $n \mid a-b$

$\cdot \equiv \cdot \pmod n$
$\Downarrow$
Congruence modulo n.

How to read

If $a \equiv b \pmod n$, then we say 'a' is congruent to 'b' modulo n or 'a' is equivalent to 'b' modulo n.

Lemma: The relation "Congruence modulo n" i.e. "$\cdot \equiv \cdot \pmod n$" is an equivalence relation on $\mathbb{Z}$.

Proof: We need to show that $\equiv \pmod n$ is reflexive, symmetric and transitive.

(i) Reflexive;

$\forall a \in \mathbb{Z}$, $a \equiv a \pmod n$ since $n \mid a-a$ or $n \mid 0$.

(ii) Symmetric

let $a \equiv b \pmod n \Rightarrow n \mid a-b$ but then $n \mid b-a \Rightarrow b \equiv a \pmod n$.

(iii) Transitive

Let $a \equiv b \pmod n$ and $b \equiv c \pmod n$

$\Rightarrow$ $n \mid b-a$ and $n \mid c-b$

$\Rightarrow$ $n \mid b-a+c-b$ $\Rightarrow$ $n \mid c-a$

$\Rightarrow$ $a \equiv c \pmod n$.

Lemma: There are exactly n equivalence classes modulo "congruence modulo n".

$$[0] = n\mathbb{Z} = \{ n \cdot m ; \ m \in \mathbb{Z} \}$$

$$[1] = n\mathbb{Z} + 1 = \{ nm + 1 ; \ m \in \mathbb{Z} \}.$$

$\vdots$

$$[a] ; \ n\mathbb{Z} + a = \{ b \in \mathbb{Z} : \frac{b-a}{n} = r \}$$

$$= \{ b \in \mathbb{Z} : b = nr + a \}$$

$$= \{ nr + a ; \ r \in \mathbb{Z} \}.$$

$\vdots$

$$[n-1] = n\mathbb{Z} + (n-1)$$

$$[n] = [0]$$

$$[n+1] = [1]$$

Notation: $\mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \}$

$= \{ \overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1} \}$

Lemma: Let $a \equiv b \pmod n$ and $c \equiv d \pmod n$

Then (i) $a + c \equiv b + d \pmod n$

(ii) $ac \equiv bd \pmod n$

Pf: $a \equiv b \pmod n \Rightarrow n \mid b - a$

$c \equiv d \pmod n \Rightarrow n \mid d - c$

(i) $\Rightarrow n \mid (b-a) + (d-c)$

$\Rightarrow n \mid (b+d) - (a+c)$

$\Rightarrow a + c \equiv b + d \pmod n.$

(ii) $n \mid b - a \Rightarrow n \mid c(b-a)$

$\Rightarrow n \mid bc - ac$ — (A)

and $n \mid d - c \Rightarrow n \mid b(d-c)$

$\Rightarrow n \mid bd - bc$ — (B)

From (A) & (B) $n \mid (bc - ac) + (bd - bc)$

$\Rightarrow n \mid bd - ac$

$\Rightarrow \quad ac \equiv bd \pmod{n}$.

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

Define $+_n$, $\cdot_n$

$+_n \downarrow$ Addition modulo n

$\cdot_n \searrow$ Multiplication modulo n

as follows;

$$\bar{i} +_n \bar{j} = \overline{i+j} \qquad [i] + [j] = [i+j]$$

$$\bar{i} \cdot_n \bar{j} = \overline{i \cdot j} \qquad [i] \cdot [j] = [i \cdot j].$$

Then $+_n$ and $\cdot_n$ are indeed well-defined.

Pf: let $\bar{i} = \bar{i'}$, $\bar{j} = \bar{j'}$

Exercise: Show that

$$\bar{i} +_n \bar{j} = \bar{i'} +_n \bar{j'}$$

and

$$\bar{i} \cdot_n \bar{j} = \bar{i'} \cdot_n \bar{j'}$$

Proposition: (1) $\bar{i} +_n \bar{j} = \bar{j} +_n \bar{i}$ (2) $\bar{i} \cdot_n \bar{j} = \bar{j} \cdot_n \bar{i}$

(3) $(\bar{i} +_n \bar{j}) +_n \bar{k} = \bar{i} +_n (\bar{j} +_n \bar{k})$ (4) $\bar{i} \cdot_n (\bar{j} \cdot_n \bar{k}) = (\bar{i} \cdot_n \bar{j}) \cdot$

(5) $\bar{0} + \bar{i} = \bar{i} = \bar{i} + \bar{0}$

(6) $\bar{1} \cdot \bar{i} = \bar{i} = \bar{i} \cdot \bar{1}$

(7) $\bar{i} + \overline{-i} = \overline{i + -i} = \bar{0}$

Def:

Let G be a set, and $*$ be a binary equation on G. ~~If the~~ The following law

① $\boxed{a * x = b * x \Rightarrow a = b}$

is called right cancellation law.

② $\boxed{y * a = y * b \Rightarrow a = b}$

is called left cancellation law.

Cancellation laws may not hold in a semigroup

Example:

①

Consider $M_2(\mathbb{R})$: the set of all 2×2 matrices over real numbers.

then $(M_2(\mathbb{R}), \cdot)$ is a semigroup.

Let

$$A = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Now

$$A \cdot A = A \cdot C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

But $A \neq C$

Example - 2 :

$(\mathbb{Z}_{15}, \cdot)$ is a semi group.

$[3] \cdot [5] = [6] \cdot [5] = [0]$

But $[3] \neq [6]$ in $\mathbb{Z}_{15}$

Note: let $(G, *)$ be a group. Let $a, b \in G$.

Consider the equations:

$$a * x = b \quad \text{and} \quad y * a = b.$$

Then $x = a^{-1} * b$ and $y = b * a^{-1}$ are the solutions.

Natural question:

Whether these statements are true in a semi-group $(G, *)$.

Example: Consider the semi-group $(\mathbb{N}, +)$.

Consider the equations

$$4 + x = 3$$
$$y + 7 = 5$$

$\Downarrow$

These equations have no solutions in $\mathbb{N}$.

Theorem: A Semigroup $(G, *)$ is a group iff $\forall\, a, b \in G$ the equations $a * x = b$ and $y * a = b$ have solutions in G.

Proof: Let $\forall\, a, b \in G$, the equations $a * x = b$ and $y * a = b$ have solutions in G.

Claim: $(G, *)$ is a group.

(i) G has an identity element.

(ii) Eeach element of G has an inverse.

(i) **Existence of identity:**

Let $m \in G$. By the assumption

$m * x = m$ and $y * m = m$ have solutions in G, say these solutions are e and e' respectively, i.e.

$$m * e = m \quad \text{and} \quad e' * m = m.$$

Again from the hypothesis

The equations $m * x = e$ and $y * m = e'$ have solutions in G.

Let ~~$y * m = e$~~ $\quad m * x = e$ —(1)

$$y * m = e' \quad \text{—(2)}$$

Now,

$$m * x = e$$

$$\Rightarrow y * (m * x) = y * e$$

$$\Rightarrow (y * m) * x = y * e$$

$$\Rightarrow e' * x = y * e$$

~~Since equations (1) & (2) have solution that is why we are able to proceed.~~

From (1)

$$m * x = e$$

$$\Rightarrow e' * (m * x) = e' * e$$

$$\Rightarrow (e' * m) * x = e' * e$$

$$\Rightarrow m * x = e' * e$$

$$= \quad e = e' * e \quad \text{From (1)} \quad \text{—(3)}$$

From (2)

$$y * m = e'$$

$$\Rightarrow (y * m) * e = e' * e$$

$$\Rightarrow y * (m * e) = e' * e$$

$$\Rightarrow y * m = e' * e$$

$$\Rightarrow e' = e' * e \quad \text{—(4)}$$

From (3) and (4) $= e = e'$.

Hence, 'e' is the required identity.

Existence of inverse

Let $m \in G$. We have to show existence of $n \in G$ s.t. $m * n = n * m = e$.

However note that

The equations

$$m * x = e \quad \text{and} \quad y * m = e \text{ have}$$

solutions in G, say those solutions are n_1 and n_2 respectively.

i.e. $m * n_1 = e$ and $n_2 * m = e$

Now,

$$\begin{aligned} n_1 = e * n_1 &= (n_2 * m) * n_1 \\ &= n_2 * (m * n_1) \\ &= n_2 * e \\ &= n_2 \end{aligned}$$

Hence, $n = n_1 = n_2$ is the required inverse.

Conversely → Exercise.

Example :

$(\mathbb{Z}_{15}, \cdot_{15})$ is a semigroup.

$\overline{3} \cdot \overline{5} = \overline{6} \cdot \overline{5} = \overline{0}$

But $\overline{3} \neq \overline{6}$.

~~However~~

Theorem: A finite semigroup in which cancellation laws hold is a group.

Proof: Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite semigroup, in which cancellation laws hold.

Claim, $(G, *)$ is a group.

(i) Existence of identity.

(ii) Existence of inverse.

Can we use previous theorem :

Consider, an equation $a * x = b$ for some $a, b \in G$.

Claim, the equation $a * x = b$ has a solution in G.

Now, consider the set $G' = \{a*a_1, a*a_2, \dots, a*a_n\}$.

Note that if $a*a_i = a*a_j$, so by cancellation laws, $a_i = a_j$.

So, no two terms among $a*a_1, \dots, a*a_n$ are repeated.

Hence, G' has n-elements, and G has also n elements.

So, $G = G'$.

So, $b \in G = G'$

$\Rightarrow b = a*a_j$ for some j.

Hence, the equation $a*x = b$ has a solution in G.

Exercise: Show that $\forall\, a, b \in G$, the equation $y*a = b$ has a solution in G.

Def: A group $(G, *)$ is called an abelian group if $\forall a, b \in G$, $a * b = b * a$.

Example: $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(M_n(\mathbb{R}), +)$
$(\mathbb{Z}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$.

Examples (non-abelian group):

$(GL_n(\mathbb{R}), \cdot)$ is not abelian.

Quaternian group, $(Q_8, \cdot)$ is not abelian.

S_n; $n \geq 3$ is not abelian.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Hence, S_3 is not abelian.

Exercise: Show that in general S_n, $n \geq 3$ is not abelian.

Notation: Let $(G, \cdot)$ be a group. For, $n \in \mathbb{N}$.

Define: $\forall x \in G$, $x^0 = e$.

$$x^n = \underbrace{x \cdot x \cdots x}_{n\text{-times}}, \quad n > 0$$

$$x^{-n} = \underbrace{(x^{-1}) \cdot (x^{-1}) \cdots (x^{-1})}_{n\text{-times}}$$

$n > 0$.

Problem: Let $(G, \cdot)$ be a group such that $\forall a \in G$, $a^2 = e$. Then G is an abelian gp.

Solution: Let $a, b \in G$.

$$(a \cdot b)^2 = e \Rightarrow (a \cdot b)(a \cdot b) = e$$
$$\Rightarrow a \cdot b = b^{-1} \cdot a^{-1}$$

However, note that if $a^2 = e$ then

$$a \cdot a = e \Rightarrow a = a^{-1}.$$

So, $ab = ba$

Hence, G must be abelian.

Problem: Let $(G, \cdot)$ be a group s.t. $\forall a, b \in G$

$(ab)^2 = a^2 b^2$. Then $(G, \cdot)$ is abelian.

Solution: $\forall a, b \in G$.

$abab = aabb$

$\Rightarrow \cancel{a}ba\cancel{b} = \cancel{a}ab\cancel{b}$

$\Rightarrow ba = ab$

$\Rightarrow G$ is abelian.

Problem: If G is a finite group, then show that there is a positive integer N such that

$a^N = e \quad \forall a \in G.$

Solution: Let $G = \{a_1, a_2, \dots, a_n\}$ be a finite group. For $a_i \in G$, consider the elements,

$a_i, a_i^2, a_i^3, \dots$

Now, since G is a group, so each of

$a_i^t \in G$,

and since G is finite, so some terms among $a_i, a_i^2, a_i^3, \ldots$ must be repeated.

$\Rightarrow$ $\exists$ t_1, t_2 s.t.

$$a_i^{t_1} = a_i^{t_2}$$

$$\Rightarrow a_i^{t_1 - t_2} = e$$

but $t_1 - t_2 = n_i$

$$\Rightarrow a_i^{n_i} = e.$$

let $N = n_1 \times n_2 \times \cdots, n_n$. Then

$$a^N = e.$$

Problem: If the group G has three elements, then show that G must be abelian.

Let $G = \{e, a, b\}$.

If $a \cdot b = a$, then $b = e$ | not possible.

If $a \cdot b = b$ then $a = e$

So $a \cdot b \neq a$, $a \cdot b \neq b$

$\Rightarrow ab = e$

Similarly, $ba = e$.

Exercise: There is only one, we can make $G = \{a, b, c\}$ into a group. ~~Hence~~

Conclude that ~~every group~~.

Exercise Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$\in S_4$.

Compute $\sigma \cdot \tau$ and $\tau \sigma$.

Exercise : Show that any group having 4-elements must be abelian.