Thm:— A finite semigroup $(S, *)$ is a group iff $(S, *)$ satisfies the cancellation laws.

$\Rightarrow$ Let $(S, *)$ satisfies cancellation laws.

for $a, b \in S$, $a * x = b$, $y * a = b$.

Let $S = \{a_1, a_2, \dots, a_n\}$.

$A = \{a * a_1, a * a_2, \dots, a * a_n\} \subseteq S$.

$[\because a * a_i \in S \; [\text{closure}]]$ $i = 1(1)n$.

Let $a * a_p = a * a_q$, for $1 \le p < q \le n$.

$\Rightarrow a_p = a_q$ [by left cancellation]

Then all elements of A are distinct.

$\therefore A = S = \{a * a_1, a * a_2, \dots, a * a_n\}$

Since $b \in S$, $b = a * a_j$, for $a_j \in S$.

$\therefore a * x = b$ has a solution a_j in S.

Illy, $y * a = b$ " " " a_k in S.

$\therefore (S, *)$ forms a group.

Conversely, if $(S, *)$ is a group, then cancellation law holds.

$a^j \; a^{i-j} \; b = a^j . b$

$\{ab, a^2b, \dots\}$

$\curvearrowright$ $a^i b = a^j b$

$a^{i-j} b = b$

i) $i - j = 1$

ii) $i - j > 1$

Order of a group :—→

Order of an element of a group :—

Let G be a group and $a \in G$. Then order of a is the least (+)ve integer n s.t. $a^n = e$.

It is denoted by $|a| = n$.

Prop:— let $|a| = n$ and $a^m = e$

$\Rightarrow n/m$ (n divides m)

$\Rightarrow |a| / m$.

Let, $m = nq + r$, $0 \le r < n$ ——— (1)

$a^m = e$

$\Rightarrow a^{nq+r} = e \Rightarrow a^{nq} \cdot a^r = e$

$\Rightarrow (a^n)^q \cdot a^r = e$

$\Rightarrow e^q \cdot a^r = e \quad [\because |a| = n]$

$\Rightarrow a^r = e \quad 0 \le r < n.$

Since n is the least (+)ve integer s.t. $a^n = e$. So only possibility is

$r = 0$

$\therefore$ From (1), $m = nq$

$\Rightarrow n/m.$

$(G, +)$ be a group. If $a \in G$ and $|a| = n \Rightarrow na = e$

Prof:— Let $(G, *)$ be a group,

$a, b \in G$ and $m, n \in \mathbb{Z}$, then,

i) $a^m * a^n = a^{m+n} = a^n * a^m$

ii) $(a^n)^m = a^{nm}$

iii) $a^{-n} = (a^n)^{-1}$

iv) $(a*b)^n = a^n * b^n$ if G is abelian.

$\Rightarrow (a*b)^n = (a*b) * (a*b) * \cdots * (a*b)$

$= a * (b*a) * (b*a) \cdots$

$= a * (a*b) \cdots$

$= (a * a * \cdots * a) * (b * b * \cdots b)$

$= a^n * b^n.$

Ex:— i) $(\mathbb{R}^*, \cdot)$ $\quad |1| = 1, \quad |-1| = 2$

counter example:— converse of (iv) is not true.

D_4, R_{90}, V

$(R_{90} \cdot V)^3 = (D)^3 = D$

$R_{90}^3 \cdot V^3 = R_{270} \cdot V = D'$

$(a \cdot b)^3 \neq a^3 \cdot b^3$

Prop:— # $a, b \in G$. If $(a*b)^n = a^n * b^n$ holds for consecutive 3 integers, then G is abelian.

H/W

Ex:— $(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{12}, +)$

$|3| = 4, \quad |6| = 2, \quad |7| = 12$

$= \frac{12}{\gcd(3,12)}$ $= \frac{12}{\gcd(6,12)}$ $= \frac{12}{\gcd(7,12)}$

$|4| = 3 = \frac{12}{\gcd(4,12)}$

$a \in \mathbb{Z}_{12}, \quad |a| = \frac{|\mathbb{Z}_{12}|}{\gcd(a,12)}$

$\int |3^2| = \frac{4}{\gcd(2,4)}$

$|9| \; |3^3| = \frac{4}{\gcd(3,4)} = 4$

$= 2$

$\# \quad |1| = 12$

$a \in \mathbb{Z}_{12}, \quad a = a.1 = 1^a$

$3 = 3.1 = 1^3 \quad (\omega.r.t. \cdot)$

$|a| = 12, \quad |a^3| = 4 = \frac{|a|}{\gcd(3,|a|)}$

$\# \quad |2| = 6,$

(3.2) $|2^3| = |6| = 2 = \frac{|2|}{\gcd(3,|2|)}$

$= \frac{6}{\gcd(3,6)} = 2$

Prop :—

Let $(G, \circ)$ be group and $a \in G$ with $|a| = n$. Then for any (+)ve integer t, $o(a^t) = \frac{n}{\gcd(t,n)}$

$\Rightarrow$ Let $o(a^t) = k$.

$\Rightarrow a^{tk} = e.$

$\Rightarrow n / tk \quad [\because |a| = n]$

$\Rightarrow tk = n.r, \quad r \in \mathbb{Z}$ —— (1)

claim :— $k = \frac{n}{\gcd(t,n)} \quad \left(k = \frac{n}{d}\right)$

Let $\gcd(t,n) = d$

$\exists$ some integers u, v s.t.

$t = du$, $n = dv$, $\gcd(u, v) = 1$.

From (1), $tk = nr$

$\Rightarrow duk = dvr$

$\Rightarrow uk = vr$

$\Rightarrow v / uk$

$\Rightarrow v / k \quad [\because \gcd(u, v) = 1]$

$\Rightarrow \frac{n}{d} / k \quad [\because n = dv]$

— (A)

$$(a^t)^{\frac{n}{d}} = a^{tn/d} = a^{dun/d} = a^{un}$$

$$= (a^n)^u = e^u = e.$$

But $o(a^t) = k$

$\therefore k / \frac{n}{d}$ — (B)

From (A), (B),

$$k = \frac{n}{d}$$

$$\Rightarrow o(a^t) = \frac{n}{\gcd(t, n)}$$