Some Properties of Groups:

Theorem 1.25: If G is a group with a binary operation $*$, then the left and right cancellation laws hold in G, that is:

(1) $a * b = a * c$ implies $b = c$

(2) $b * a = c * a$ implies $b = c$

For all $a, b, c \in G$.

Proof: (Home Work).

Theorem 1.26: In a group $(G, *)$, there is only one element e in G such that $e * a = a * e = a$, $\forall a \in G$.

Proof: Suppose that G has two identity elements e and e' that mean $\forall a \in G$.

$a * e = e * a = a$ and $a * e' = e' * a = a$

Since each e and e' belong to G, so

$e * e' = e' * e = e$ (e عنصر و e' عنصر محايد)

$e' * e = e * e' = e'$ (e' عنصر و e عنصر محايد)

It follows that $e' = e$.

Theorem 1.27: In a group $(G, *)$, the inverse element of each element in G is unique.

Proof: Let $a \in G$ and a has two inverse x and x'. Such that

$a * x = x * a = e$

$a * x' = x' * a = e$

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

$\therefore x = x' \Rightarrow$ the inverse is an unique element.

Theorem 1.28: If $(G , *)$ is group , then

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

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

(3) $(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall \quad a , b \in G$

Proof:

(1) Let $e^{-1} = x$

e is the identity element of G $\Longrightarrow x * e = e * x = x$ ------- (1)

x is the inverse of e $\Longrightarrow e * x = x * e = e$ ------- (2)

from (1) and(2) $\Longrightarrow x = e \Rightarrow e^{-1} = e$.

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

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

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

$= e * a = a.$

(3) To prove, $(a * b)^{-1} = b^{-1} * a^{-1}, \quad \forall\ a , b \in G$

Since $(a * b) \in G \Longrightarrow (a * b)^{-1} \in G$

$(a * b) * (a * b)^{-1} = (a * b)^{-1} * (a * b) = e$ (def . of inverse)

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

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

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

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

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

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

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

Theorem 1.29: Let $(G , *)$ be a group . Then

(1) $(a * b)^{-1} = a^{-1} * b^{-1} \Leftrightarrow$ G is comm. group.

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: (1) ($\Longrightarrow$) Let $(G , *)$ be a group and $(a * b)^{-1} = a^{-1} * b^{-1}$.

To prove G is comm.

Let $a , b \in G$. To show $a * b = b * a , \forall\ a , b \in G$

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

$= (b^{-1} * a^{-1})^{-1}$ (by Theorem 1.29 (3))

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

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

$\therefore$ G is comm. gp.

($\Leftarrow$) Let $(G , *)$ is a comm . gp.

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

$(a * b)^{-1} = b^{-1} * a^{-1}$ (by Theorem 1.28 (3))

$= a^{-1} * b^{-1}$ (by comm.)

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: Let $a = a^{-1}$ To prove, $a * b = b * a$, $\forall a , b \in G$

Let $a , b \in G$ and $a * b \in G \Longrightarrow (a * b) = (a * b)^{-1}$

$= b^{-1} * a^{-1}$ (by Theorem 1.29 (3))

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

$\therefore$ G is a comm. Group.

The converse of this part is not true.

(i.e.) if $(G , *)$ is comm . $\nRightarrow a = a^{-1}$

For example:

Let $(G = \{1, -1, i, -i\}, .)$ be comm . group,

Let $a = i \Longrightarrow a^{-1} = -i$

$\therefore a \neq a^{-1}$

Give another example **(Home Work).**

Definition 1.30: (**The Integral Powers of *a***)

Let $(G , *)$ be a group . The integral powers of a, $a \in G$ is defined by :

(1) $a^n = \underbrace{a * a \ldots * a}_{n-times}$

(2) $a^0 = e$

(3) $a^{-n} = (a^{-1})^{n}, n \in Z^+$

(4) $a^{n+1} = a^{n} * a \ , n \in Z^+.$

For example 1.31:

(1) In $(R , +)$,

$3^0 = 0$,

$3^3 = 3 + 3 + 3 = 9$,

$3^{-2} = (3^{-1})^{2} = (-3) + (-3)$

$= -6$.

(2) In (R , .) ,

$2^0 = 1$,

$2^3 = 2 \times 2 \times 2 = 8$,

$2^{-4} = (2^{-1})^4 = (\frac{1}{2})^4$

$= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16}$

(3) In (G = {1, -1, i, -i}, .) ,

$i^o = 1$, $i^2 = i \times i = -1$, $i^{-2} = (i^{-1})^2 = (-i)^2 = - i \times -i = -1$

Theorem 1.32: Let $(G , *)$ be agroup and $a \in G$, $m , n \in Z$, then :

(1) $a^n * a^m = a^{n+m}$ $\forall n , m \in Z$ (H. W.)

(2) $(a^n)^m = a^{n\,m}$ $\forall n , m \in Z^+$

(3) $a^{-n} = (a^n)^{-1}$ $\forall n \in Z^+$

(4) $(a * b)^n = a^n * b^n$ $\forall n \in Z \Leftrightarrow$ G is comm . group.

Proof:

(2) To prove, $(a^n)^m = a^{n\,m}$, $\forall n , m \in Z^+$

Let p(m) : (($(a^n)^m = a^{n\,m}$ $\forall n \in Z^+$))

To prove, P(m) is true $\forall m \in Z^+$

If $m = 1 \Longrightarrow p(1) : (a^n)^1 = a^n = a^{n \times 1} \Longrightarrow$ p(1) is true

Suppose that p(k) is true with $k \in Z^+$ and $k \leq m$

$\therefore (a^n)^k = a^{nk}$

We have to prove that p (k + 1) is true P (k+ 1) : $(a^n)^{k+1} = a^{n(k+1)}$??

$(a^n)^{k+1} = (a^n)^k * (a^n)^1$ (by define of $a^{n+1} = a^n * a^1$)

$= a^{nk} * a^n$

$= a^{nk+n}$ by (1) above

$= a^{n(k+1)}$

$\therefore$ p (k + 1) is true

By the principle of mathematical induction

$\Longrightarrow$ p (m) is true $\forall m \in Z^+$

$\therefore (a^n)^m = a^{nm}$, $\forall n , m \in Z^+$