Group Theory

Definition:

Let S be a non empty set, any functionform the Cartesian product $S \times S$ into S is called a binary operation on S.

Definition:

If $*$ is binary operation on a set S and $A \subseteq S$, the subset A is closed under $*$ if $a * b \in A$, where a and b are in A.

Examples:(1)on $Z, +$

$$+: Z \to Z; +(a, b) = a + b$$
$$Z \to Z; \cdot (a, b) = a \cdot b$$

also is a binary operation
(2) If $P(A)$ is denoted the power set of fixed set A, then both u, n are binary operation on $p(A)$.
(3) On^{+}, the subtraction is not closed on Z^{+}
(4) $S = \{1, -1, i, -i\}$ with $i^2 = -1$, then - is a binary operation on S
(5) $(Z_e, +)$ is a group under a binary operation +
$(Z_0, +)$ is not closed under addition

Definition:

A group is a pair $(G,*)$ consisting of nonempty set G and a binary operation $*$ define on G satisfying.
$1 - G$ closed under operation*.
2-*Is associative $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
3-There exist $e \in G$ (the identity element) such that $a * e = e * a = a$, for all $a \in G$
4-For all $a_{\in} G$ there exists an inverse a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Definition:

The binary operation * on set S is called commutative if $a * b = b * a$.

Examples:

1- $(Z,+),(R,+),(C,+)$ Are associative groups.
2-Let a be any non zero real number $0 \neq a \in R, G = \{na : n \in Z\}$,
$(G,+)$is group
3- $(P(A),\text{n}),(P(A),\cup$ are not groups.
Solution:

$$A \cup \phi = A$$
$$A \cap X = A$$

But the system has no invers.
Thus we define other operation,

$$A\Delta B = (A - B) \cup (B - A); A, B \in P(A)$$
$$A\Delta\phi = (A - \phi)_{\cup}(\phi - A) = A_{\cup}\phi = A$$
$$A\Delta A = (A - A)_{\cup}(A - A) = \phi_{\cup}\phi = \phi$$

Thenall $A \in P(A)$ has inverse. So $(P(A),\Delta)$ is group

Definition:

Let $(G,*)$ be a group, G is called abelian group if $a * b = b * a$ for all a, b in G

Example:

$(P(A),\Delta)$ and $(Z,+)$ are abeliangroup.

Examples:

(1) Let $G = \{(a,b) : a, b \in R, a \neq 0\}$.Define* on G as:
$(a,b) * (c,d) = (ac, bc + d), (G,*)$ is group.
Sol:
*isassociative
(1,0) identity
$\left(\frac{1}{a}, \frac{-b}{a}\right)$ is the inverse of (a,b)
But $(G,*)$ is not abelian since

$$(1,2) * (3,4) = (3,10)$$
$$(3,4) * (1,2) = (3,6)$$

(2) Let G be a group, let $H = \{a, b \in G : a \times b = e\}$.
$(H,\times)$ is not group.
(3) Let

$$G = \{fi : R - \{0,1\} \to \{0,1\}\}, i =$$
$$1,2,3,4,5,6 \text{ where } f_1(x) = x, f_2(x) = \frac{1}{x}, f_3(x) = 1 -$$
$$x, f_4(x) = \frac{1}{1-x}, f_5(x) = \frac{x-1}{x}, f_6(x) = \frac{x}{x-1}, \text{ then}$$

$(G,\circ)$ is group

Remarks:

-1. Let Gbe a group then the identity is unique $\mathrm{e}_1 = \mathrm{e}_1 * \mathrm{e}_2 = \mathrm{e}_2$.
2. Let G be a group and $a \in G$, then a^{-1} is unique.
3. Let G be a group and $\in G$, then $(a^{-1})^{-1} = a$.

Proof (1): Suppose e_1 and e_2 both identity in G $e_2 = e_1$ (sincee e_1 identity) $* e_2$ (since e_2 identity) $= e_1$
$\therefore e_1 = e_2$
Proof (2): Suppose b_1 and b_2 are inverse of a

$$a * b_1 = b_1 * a = e$$
$$a * b_2 = b_2 * a = e$$
$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

Proof (3): a inverse of a^{-1}
$(a^{-1})^{-1}$ inverse of a^{-1}
But the inverse is unique
$\therefore a = (a^{-1})^{-1}$

Remark:

Let G be a group and $a, b \in G$, then $(\mathrm{a} * \mathrm{b})^{-1} = b^{-1} * \mathrm{b}^{-1}$

Proof: $(\mathrm{b}^{-1} * \mathrm{a}^{-1}) * (\mathrm{a} * \mathrm{b}) = \mathrm{b}^{-1} * (\mathrm{a}^{-1} * \mathrm{a}) * \mathrm{b} = \mathrm{b}^{-1} * \mathrm{e} * \mathrm{b} = \mathrm{b}^{-1} * \mathrm{b} = \mathrm{e}$
$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$
Thus $b^{-1} * a^{-1}$ is inverse of $a * b$ but
$(a * b)^{-1}$ is inverse of $a * b$ by (b)

the inverse unique
thus $(a*b)^{-1} = b^{-1} * a^{-1}$

Theorem:

(Cancellation law): Let G be a group and $a, b, c \in G$
(1) If $a * b = a * c$, then $b = c$.
(2) If $b * a = c * a$, then $b = c$.
Proof(1):
$a^{-1} * (a * b) = a^{-1} * (a * c)[a^{-1} \in G$, since G is a group]
$(a^{-1} * a) * b = (a^{-1} * a) * c$ [*Associative, since G is a group]
$e * b = e * c$
$b = c$

Definition:

Let G be a group and $a \in G, n$ any positive integer

$$a^{n} = \underbrace{a * a * \ldots * a}_{\text{n times}}$$

Remark:

Let $(G,*)$ be a group and $a \in G$, then for all $n, m \in Z$
$1 - a^{n+m} = a^{n} * a^{m}$
$2 - (a^{n})^{m} = a^{nm}$

Problems:

(1) Determine whether or not the following are abelian groups
a. $G = Q - \{1\}: a * b = a + b - ab$.
b. $G = R \times R: (a, b) * (c, d) = (ac - bd, ad + bc)$.
c. $G = Z: a * b = 0$

Proof(a):

- Is a binary operation

If $a + b - ab = 1\,; a, b \in Q - \{1\}$
Then $b(1 - a) = 1 - a$, then $b = 1$ contradiction

$*$ Is associative .
Let $a, b, c \in Q - \{1\}$, we want to show that $(a * b) * c = a * (b * c)$

$$(a + b - ab) * c = a * (b + c - bc)$$

L.H.S. $= a + b - ab + c - ac - bc + abc$
R.H.S. $= a + b + c - bc - ab - ac + abc$,

The identity $e = 0, a \in G$

$$a * 0 = a + 0 - a.0 = a$$
$$0 * a = 0 + a - 0a = a$$

Let $b \in G$, suppose there is y then $b * y = 0$ and $b + y -$ by $= 0$
Then $y(1 - b) = -b, y = b/b - 1 \in Q - \{1\}$
If $b/b - 1 = 1$, then $b = b - 1$, then $1 = 0$ contradiction Hence $b = 1b^{-1} =. b/b - 1$
Thus $(G,*)$ is a group.
Now, since $a * b = a + b - ab, b * a = b + a - ba$, then $a * b = b * a$
Thus ($G,*$) is anabelain) group.
2- Let$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where $f_i: R - \{0\} \to R - \{0\}$ define by

$$f_1(x) = x, f_2(x) = \frac{1}{x}, f_3(x) = 1 - x, f_4(x) = \frac{1}{1-x}, f_5(x) = \frac{x-1}{x}, f_5(x) = \frac{x}{x-1}.$$

Is $(G,\circ)$ Abelian group? Why?.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_1	f_5	f_3