Result 5 In a group $(G, \circ)$, (i) $(a^{-1})^{-1} = a$ (ii) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Proof: (i) As for each $a \in G$ $a \circ a^{-1} = a^{-1} \circ a = e$, e is the identity element in G,

So, $(a^{-1})^{-1} = a$

(ii) ~~Now~~ Let $a, b \in G$. Then $a^{-1}, b^{-1}, a \circ b, b^{-1} \circ a^{-1}$ all belong to G.

Now $(b^{-1} \circ a^{-1}) \circ (a \circ b) = [b^{-1} \circ (a^{-1} \circ a)] \circ b$, since $\circ$ is associative

$= (b^{-1} \circ e) \circ b = b^{-1} \circ b = e$, e is the identity element in G.

Again $(a \circ b) \circ (b^{-1} \circ a^{-1}) = [a \circ (b \circ b^{-1})] \circ a^{-1}$, since $\circ$ is associative

$= (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$

So, we have $(b^{-1} \circ a^{-1}) \circ (a \circ b) = (a \circ b) \circ (b^{-1} \circ a^{-1}) = e$.

So, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Some more examples: 1. Let $\mathbb{Z}$ be the set of all integers.
We know that $(\mathbb{Z}, +)$ is a commutative group.
Let, for some positive integer m, $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$
Then we show that $(m\mathbb{Z}, +)$ is a commutative group

as (i) Let $a, b \in m\mathbb{Z}$. Then $a = mp$ and $b = mq$ for some $p, q \in \mathbb{Z}$ $a + b = m(p+q) \in m\mathbb{Z}$ as $p + q \in \mathbb{Z}$. This shows that $m\mathbb{Z}$ is closed under $+$

(ii) Addition $+$ is associative in $\mathbb{Z}$ and $m\mathbb{Z}$ is a subset of $\mathbb{Z}$. So, addition is associative in $m\mathbb{Z}$

(iii) $0 = m.0 \in m\mathbb{Z}$ and $a + 0 = 0 + a = a$ for all $a \in m\mathbb{Z}$
So, 0 is the identity element.

(iv) Let $a \in m\mathbb{Z}$ and $a = mp$ Then $-a = -mp = m(-p) \in m\mathbb{Z}$
and $a + (-a) = (-a) + a = 0$. So, $-a$ is the inverse of a.

(v) Addition is commutative binary operation on $\mathbb{Z}$ and $m\mathbb{Z}$ is a ~~sub~~ subset of $\mathbb{Z}$. So addition is commutative on $m\mathbb{Z}$.

Scanned with CamScanner

If we take $n=2$, then $2\mathbb{Z}$ = the set of all even integers also form a commutative group with respect to $+$.

If we take $n=3$, then $3\mathbb{Z}$ = the ~~set~~ set of all integers which are multiple of 3 also forms a commutative group with respect to $+$.

Note: In a group (G, o), $e^{-1} = e$, e being the identity element in G as $eoe = eoe = e$.

Definition: An element a in ~~a~~ a group (G, o) is said to be an idempotent element if $aoa = a$

we prove that the identity element e is the only idempotent element in a group (G, o).

Let a be an ~~ident~~ idempotent element in (G, o)

Then $aoa = a$ or $aoa = aoe$ (as $aoe = a$)

So, by left cancellation law, $a = e$. So e is the only idempotent element in G.

~~Some~~ Some problems

1. Examine if the following systems are groups:

(i) $(\mathbb{Z}, o)$ where $aob = a+b+1$, $a, b \in \mathbb{Z}$

(ii) $(\mathbb{Z}, o)$ where $aob = a+b+ab$, $a, b \in \mathbb{Z}$

(iii) $(\mathbb{R}^*, o)$ where $aob = |ab|$, $a, b \in \mathbb{R}^* = \mathbb{R} - \{0\}$

(iv) $(\mathbb{R}, o)$ where $aob = 2(a+b)$, $a, b \in \mathbb{R}$

($\mathbb{Z}$ is the set of all integers and $\mathbb{R}$ is the set of all real numbers)

Solution:

(i) Let $a, b \in \mathbb{Z}$. As $aob = a+b+1$, so $aob \in \mathbb{Z}$ as $a+b$ and 1 are integers. (i.e., o is a binary operation on $\mathbb{Z}$).

Let $a, b, c \in \mathbb{Z}$. Then

$(aob)oc = (a+b+1)oc = a+b+1+c+1 = a+b+c+2$ (as addition is commutative in $\mathbb{Z}$)

Also $ao(boc) = ao(b+c+1) = a+b+c+1+1 = a+b+c+2$

So, $ao(boc) = (aob)oc$, So o is associative.

Now, $-1 \in \mathbb{Z}$ and $a \circ (-1) = a + (-1) + 1 = a$ for any $a \in \mathbb{Z}$

Also $(-1) \circ a = -1 + a + 1 = a$, for any $a \in \mathbb{Z}$

So, $a \circ (-1) = (-1) \circ a = a$. So, -1 is the identity element

Now let $a \in \mathbb{Z}$ Then $a \circ (-a-2) = a + (-a-2) + 1$
$= -1$

Also, $(-a-2) \circ a = -a-2+a+1 = -1$

Hence $-a-2$ is the inverse of a in $\mathbb{Z}$

So, $(\mathbb{Z}, \circ)$ is a group.

(ii) Let $a, b \in \mathbb{Z}$ Here $a \circ b = a+b+ab \in \mathbb{Z}$ as $a+b$ and $ab \in \mathbb{Z}$.

Now $(a \circ b) \circ c = (a+b+ab) \circ c = a+b+c+ab+ac+bc+abc$

Also $a \circ (b \circ c) = a \circ (b+c+bc) = a+b+c+ab+ac+bc+abc$

So, $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in \mathbb{Z}$

So, $\circ$ is associate

Let $a \in \mathbb{Z}$

Now $a \circ 0 = 0 \circ a = a$ $\forall a \in \mathbb{Z}$. So 0 is the identity element

Now ~~for a ...~~ for $4 \circ a = 0$, we have

$4 + a + 4a = 0$

or, $5a = -4$ or, $a = -\frac{4}{5} \notin \mathbb{Z}$

So 4 has no inverse in $\mathbb{Z}$

So, $(\mathbb{Z}, \circ)$ is not a group

(iii) Let $a, b \in \mathbb{R}^*$. So, $a \neq 0$, $b \neq 0$. So $ab \neq 0$

So, $a \circ b = |ab| \neq 0$ and $|ab| \in \mathbb{R}$

So, $a \circ b \in \mathbb{R}^*$

Now $a \circ (b \circ c) = a \circ |bc| = |a|bc|| = |abc|$

Also $(a \circ b) \circ c = |ab| \circ c = ||ab|c| = |abc|$

So, $(a \circ b) \circ c = a \circ (b \circ c)$. So, $\circ$ is associative

If possible, let e be the identity in G. Then for $a \in \mathbb{R}^*$

$a \circ e = a \Rightarrow |ae| = a$. As $a \neq 0$, $e \neq 0$

we have, either $ae > 0$ or $ae < 0$

If $ae > 0$ then $|ae| = a \Rightarrow ae = a \Rightarrow e = 1$

If $ae < 0$ then $|ae| = a \Rightarrow -ae = a \Rightarrow e = -1$

So, that we see that $-3 \circ 1 = |-3 \times 1| = 3 \neq -3$

and $-3 \circ -1 = |-3 \times (-1)| = 3 \neq -3$

So, there is no identity in $\mathbb{R}^*$

So, $(\mathbb{R}^*, \circ)$ is not a group.

(iv) Let $a, b \in \mathbb{R}$. Then $a \circ b \in \mathbb{R}$ as $a \circ b = 2(a+b)$

and as $a+b \in \mathbb{R}$ and $2 \in \mathbb{R}$ $a \circ b \in \mathbb{R}$

~~$a \circ (b \circ c) = a \circ (2(b+c)) = 2(a+2(b+c)) =$~~

now $1 \circ (2 \circ 3) = 1 \circ (2(2+3)) = 1 \circ 10 = 2(1+10) = 22$

and $(1 \circ 2) \circ 3 = (2(1+2)) \circ 3 = 6 \circ 3 = 2(6+3) = 18$

So, $1 \circ (2 \circ 3) \neq (1 \circ 2) \circ 3$. So, $\circ$ is not associative

So, $(\mathbb{R}, \circ)$ is not a group.

2. Prove that the set of all complex numbers of unit modulus forms a commutative group with respect to multiplication.

Proof: Let $G = \{z : z \text{ is a complex number and } |z| = 1\}$. We have to show that G is a group with respect to multiplication.

Let $z_1, z_2 \in G$ then $|z_1| = 1$ and $|z_2| = 1$. So, $|z_1 z_2| = |z_1||z_2| = 1$

So, $z_1 z_2 \in G$. As $z \in G$ is a complex number and $|z| = 1$

we write $z = \cos\theta + i\sin\theta$. Here $1 \in G$ and $z \cdot 1 = 1 \cdot z = z$

for all $z \in G$. So, 1 is the identity element in G.

If $z \in G$ and $z = \cos\theta + i\sin\theta$ Then if we take

$z' = \cos\theta - i\sin\theta$, then $z' \in G$ and $z \cdot z' = z' \cdot z = 1$. So

z' is the inverse of z. Hence G is a commutative group with respect to multiplication as complex multiplication is commutative.

Scanned with CamScanner