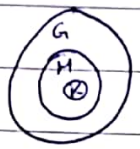
7/8/18

Subgroup.

A subset H of a group G is said to be a subgroup of a group if H itself is a group with respect to same operation defined on G.



If K is a subgroup of H and H is a subgroup of group G then K is also a subgroup of G.

Example: Let G be a group of integers.

$H = \{5m \mid m \in G\}$

H is a subgroup of G.

Theorem A non-empty subset H of the group G is a subgroup of G if and only if

1. $a, b \in H \Rightarrow a * b \in H$ (Closure).
2. $a \in H \Rightarrow a^{-1} \in H$. (Inverse).

Proof:- If H is a subgroup of G $\Rightarrow$ H is a group with $*$.

$\Rightarrow$ (1) and (2) follows.

If H is a subset of G and (1) and (2) are holding,

If $a \in H \Rightarrow a^{-1} \in H$ (by 2)

$\Rightarrow a * a^{-1} \in H$ (by 1).

$\Rightarrow e \in H$. (Identity).

__/__/____

Theorem :- If H is a non-empty finite subset of a group G and H is closed under the operation, then H is a subgroup of G.

finite H, closure in H $\longrightarrow$ Inverse in H $\longrightarrow$ H is a subgroup of G.

Proof :- Suppose $a \in H$, then $a^2 = a*a$, $a^3 = a*a*a \ldots \in H$ (H is closed).

Thus this entire collection will fit into H which is a finite subset of H. $\Rightarrow$ There must be repetition in the collection of elements, i.e.

for some integers r, s with $r > s > 0$,

$$a^r = a^s.$$

Now, $a^r, a^s \in G$ (Since $H \subset G$).

Since G is a group, cancelation property holds in G.

$$a^r * a^{-s} = a^s * a^{-s}$$

$$\Rightarrow a^{r-s} = e. \quad (e \in G) \Rightarrow e \in H.$$

Now, $r - s \geq 1 \Rightarrow r - s - 1 \geq 0$.

$$a^{r-s-1} * a = e \Rightarrow \boxed{a^{-1} = a^{r-s-1}}$$

$\therefore a^{-1} \in H$ (Inverse exists).

8) Let G be a group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad-bc \neq 0$ under matrix multiplication.

Show that $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid ad \neq 0 \right\}$ is a subgroup of G.

Ans)

Closure

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} * \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} ae & af+bg \\ 0 & dg \end{pmatrix} \in H.$$

$aedg \neq 0$ [$\because ad \neq 0$ & $eg \neq 0$].

Inverse

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} * \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$ ← Identity of G

$\therefore$ $ae = 1$, $dg = 1$, $af + bg = 0$

$e = \frac{1}{a}$ $\quad g = \frac{1}{d}$ $\quad af = -bg$

$f = -\frac{b}{ad}$.

$\therefore \begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ $\in H$.

[Proved].

__/__/____

Definition :- Let G be a group, H is a subgroup of G. for $a, b \in G$, we say a is congruent to b written as $a \equiv b \bmod H$ if $a * b^{-1} \in H$.

Theorem : The relation $a \equiv b \bmod H$ is an equivalence rel^n.

Equivalence rel^n $\Rightarrow$ Reflexive, Symmetric, Transitive.

Reflexive

$a * a^{-1} = e \in H \cdot \forall\, a \in G$.

$\boxed{a \equiv a \bmod H}$

Symmetric

If $a * b^{-1} \in H$ (i.e. $a \equiv b \bmod H$)

$\Rightarrow (a * b^{-1})^{-1} \in H$

or, $b * a^{-1} \in H$.

$\boxed{b \equiv a \bmod H}$

Transitive

If $a * b^{-1} \in H$, $b * c^{-1} \in H$ (i.e. $a \equiv b \bmod H$, $b \equiv c \bmod H$)

$\Rightarrow a * b^{-1} * b * c^{-1} \in H$

or, $a * c^{-1} \in H$

$\Rightarrow \boxed{a \equiv c \bmod H}$

__/__/____

8) Show that the intersection of 2 subgroups of a group $(G, *)$ is also a subgroup of G.

Let A, B be 2 subgroups of G.

Let $a, b \in A \cap B \Rightarrow a, b \in A$ & $a, b \in B$.

$\therefore a * b \in A$, $a * b \in B \Rightarrow a * b \in A \cap B$ (closure)

Let $a \in A \cap B \Rightarrow a \in A$, $a \in B$

$\therefore a^{-1} \in A$, $a^{-1} \in B \Rightarrow a^{-1} \in A \cap B$. (Inverse)

[Proved].

9) Show that the union of 2 subgroups of a group $(G, *)$ is a subgroup if one is contained in the other.

Let A, B be 2 subgroups of G.

Let $A \setminus B \neq \phi$ and $B - A \neq \phi$

Let $a \in A \setminus B$ and $b \in B \setminus A$.

Then, we can't definitely say $a * b \in A \cup B$.

$\therefore$ If $\exists$ any element $x \in A \setminus B$, $A \cup B$ might not be a subgroup.

10/8/16

Cyclic Group

If the elements of a group are generated by a single element 'a', by composition, then the group is said to be cyclic.

'a' is called the generator of the group.

Q) Show that all cyclic groups are abelian groups.

Let a^i, a^j be any 2 elements of a cyclic group $(G,*)$ with a as the generator. for $i,j \in Z^+$.

$$a^i * a^j = a^{i+j}$$

Also, $a^j * a^i = a^{j+i} = a^{i+j}$ (since add^n is commutative for $\geq$)

Hence, it is commutative as well.

∴ All cyclic groups are abelian.

Q) Show that if a is a generator of a cyclic group, then a^{-1} is also a generator.

DIY

Let the group be $(G,*)$ with a as the gen.

∴ Identity element $e = a^n$ where n is the order

∴ $a^{-1} = a^{n-1}$.

∴ $(a^{-1})^n = (a^{n-1})^n = a^{(n(n-1)\%n)+1}$

__/__/____

Def^n. If H is a subgroup of G and $a \in G$, then $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G.

If $a \in H$, right coset would be H itself.

Similarly, $aH = \{ah \mid h \in H\}$ is called the left coset of H in G.

Q) For all $a \in G$, show $Ha = \{x \in G \mid a \equiv x \bmod H\}$

$[a]$ congruence class of a ; $ax^{-1} \in H$.

$Ha = \{ha \mid h \in H\}$.

Now, by the given def^n, ~~$ha = x$ for some $h \in H, x \in G$~~

$\therefore h = xa^{-1}$

To show :- $Ha = [a]$.

① $Ha \subset [a]$.

Let $ha \in Ha$

To Show : $ha \in [a]$.

$\therefore a(ha)^{-1}$ must belong to H. $\Rightarrow a(a^{-1}h^{-1})$

$\therefore (aa^{-1})h^{-1}$ which is h^{-1}, which $\in H$.

__/__/____

$\therefore a(ha)^{-1} \in H$.

$\therefore ha \in [a]$.

$\therefore Ha \in [a]. \Rightarrow Ha \subset [a]$ —①.

② $[a] \subset Ha$.

Let $x \in [a]$.

To show: $x \in Ha$.

Now, $x \in [a] \Rightarrow ax^{-1} \in H$.

$\Rightarrow (ax^{-1})^{-1} \in H \Rightarrow xa^{-1} \in H$.

$\therefore xa^{-1} = h_k$ for some $h_k \in H$.

or, $x = h_k a$

$\Rightarrow x \in Ha. \Rightarrow [a] \subset Ha$ —②

① & ② $\Rightarrow Ha = [a]$.

Def^n :- If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G, and is denoted by $i_G(H)$.

Theorem If G is a finite group and H is a subgroup of G, then order $O(H)$ of H is a divisor of order $O(G)$ of G. $[i_G(H) = O(G)/O(H)]$

Proof: Let $r = O(H)$

$\therefore H = \{h_1, h_2, \ldots, h_r\}$

Trivial case: $O(G) = O(H) \Rightarrow$ It divides $O(G)$

Non-trivial case: $O(G) > O(H)$.

There must be atleast 1 element, say a, $a \in G$ s.t. $a \notin H$.

Now, $Ha = \{h_1a, h_2a, \ldots, h_ra\}$

Also, $a \in Ha$ [since $e \in H$]

① To show: $h_ia \neq h_j \ \forall\ i,j$

For $h_ia = h_j$ to be true, $a = h_i^{-1}h_j \in H$

But $a \notin H$

$\therefore h_ia \neq h_j \ \forall\ i,j$.

② To show: $h_ia \neq h_ja \ \forall\ i,j$.

By cancellation, $h_i = h_j$ which is false.

$\therefore h_ia \neq h_ja \ \forall\ i,j$

$\therefore$ For an extra element a, we get r more elements.

$\therefore$ For every extra element, r more elements will have to be present.

~~∴ r is a divisor of o(G).~~

Let $b \in G$ ~~which~~ st $b \notin H, Ha$.

① $hi\,a \neq hj\,b$
② $hi\,b \neq hj\,b$
③ $hi\,b \neq hj$.

} can be shown

∴ Another r elements ~~abc~~ should be present -

① $\Rightarrow hj^{-1}\,hi\,a = b \Rightarrow b \in Ha$ CONTRADICTION.

Def^n:- A subgroup **N** of G is said to be a normal subgroup of G, if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

i.e., if $gNg^{-1} = (gng^{-1} \mid n \in N)$, for any $g \in G$, $gNg^{-1} \subset N$.

Theorem:- N is a normal subgroup of G iff $gNg^{-1} = N$ for any $g \in G$.

Proof:- $gNg^{-1} \subset N$ follows by definition.

To show: $N \subset gNg^{-1}$. for $g \in G$

Let $n \in N$

To show: $n \in gNg^{-1}$. for $g \in G$.

__/__/____

Let $x = g * n \cdot \in G$.

$\therefore (gx^{-1})^{-1} \in N \quad [\because Hg = [g]]$.

i.e. $g(gx)^{-1}$

$gxg^{-1} \qquad xg^{-1} \in N$

$\therefore gng^{-1} \in N$

$g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \quad [\because g \in G \Rightarrow g^{-1} \in G]$.

$g^{-1}Ng \subset N$ (by defⁿ).

$N = gg^{-1}Ngg^{-1} \subset gNg^{-1}$.

$N \subset gNg^{-1}$.

14.8.18.

Theorem The subgroup N of G is a normal subgroup of G if every left coset of N in G is a right coset of N in G.

Let N be a subgroup of G.

~~Left cosets~~ :

If N is a normal subgroup of G, $gNg^{-1} = N$.

$$(gNg^{-1})g = Ng$$
$$gN(g^{-1}g) = Ng$$
$$gN = Ng$$

Now, assuming that every left coset = right coset.
Prove N is a normal subgroup.

#

Suppose N is a normal subgroup of G and $a, b \in G$.
Consider $(Na)(Nb) = N(aN)b = N(Na)b$
$= N^2ab = Nab$ [$\because N$ is closed]

Product of 2 right cosets = Right coset of product.

Q) Let G/N denote the collection of right cosets of N in G and the operation is defined as $(Na)\cdot(Nb) = Nab$.
Show that $(G/N, .)$ is a group.

Closure

Let $Na, Nb \in G/N$.

$(Na)\cdot(Nb) = Nab = N(ab) = Nc$ [since G is closed, Let $c = ab$, $c \in G$]

$\therefore Nc \in G/N$, $(Na)\cdot(Nb) \in G/N$. [Proved]

Sreya Mittal

__/__/____

Identity

Let e be the identity of G.

Let $a \in G$.

$\therefore (Na)\cdot(Ne) = Nae = Na$

$\therefore Ne$ is the identity element of G/N & it exists.

Associative

Let $a, b, c \in G$.

$(Na)\cdot((Nb)\cdot(Nc)) = Na\,Nbc = Nabc = Nab\,Nc$

$= ((Na)\cdot(Nb))\cdot(Nc)$.

Inverse

Let $a \in G$.

$\therefore Na \in G/N$.

Let Nx be the inverse of Na.

Now, $(Na)\cdot(Nax) = Ne$

$\therefore Nax = Ne$

$\therefore ax = e \Rightarrow x = a^{-1}$

since a^{-1} exists in G, Na^{-1} exists in G/N & is the inverse of Na.

Defn This is called Quotient Group.

__/__/____

Homomorphism

Def^n. A mapping ϕ from a group $(G, *)$ into a group $(\bar{G}, \circ)$ is said to be homomorphism if for all $a, b \in G$.

$$\phi(a * b) = \phi(a) \circ \phi(b).$$

Q) Tell which are homomorphisms.

i) $(\mathbb{Z}, +) \xrightarrow{\phi} (\mathbb{Z}, +)$

$\phi(x) = 2x \quad \forall \; x \in \mathbb{Z}$.

YES.

$\phi(x+y) = 2(x+y) = 2x+2y$
$= \phi(x) + \phi(y)$.

2) G be a group of all nonzero real numbers under multiplication.

$\bar{G} = \{1, -1\}$.

Operation $\circ$: $(1)\circ(1) = 1$, $(1)\circ(-1) = (-1)\circ(1) = -1$,
$(-1)\circ(-1) = 1$.

$$\phi(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0. \end{cases}$$

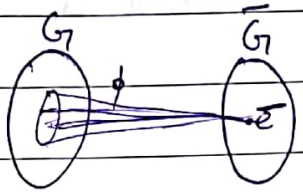
YES.

$$\phi(x * y) = \begin{cases} \text{Both +ve,} & 1 = (1)\circ(1) \\ \text{Both -ve,} & 1 = (-1)\circ(-1) \\ \text{One +ve, one -ve,} & -1 = (1)\circ(-1) \\ & -1 = (-1)\circ(1). \end{cases}$$

__/__/____

Def^n. If ϕ is a homomorphism of G into $\bar{G}$, the kernel of ϕ is defined by $K\phi$.

$$K\phi = \{ x \in G \mid \phi(x) = \bar{e},\ \bar{e} \text{ identity element of } \bar{G} \}$$



Q) If $\phi \in G \to \bar{G}$.

Prove :

① $\phi(e) = \bar{e}$.

② $\phi(x^{-1}) = \{\phi(x)\}^{-1}$.

Ans) ① $\phi(a * e) = \phi(a) \circ \phi(e)$

$\Rightarrow \phi(a) = \phi(a) \circ \phi(e)$.

$\Rightarrow \phi(a)\,\bar{e} = \phi(a) \circ \phi(e)$

$\therefore \phi(e)$ is identity of $\bar{G}$.

② $\phi(x * x^{-1}) = \phi(x) \circ \phi(x^{-1})$

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

$\therefore \phi(x^{-1}) = \{\phi(x)\}^{-1}$.

__/__/____

Q) If $\phi : G \to \bar{G}$, with kernel K, then show that K is a normal subgroup of G.

Ans) K is a subset of G.

1st we need to show that it is a subgroup.

Closure

Let $k_1, k_2 \in K$.

$\phi(k_1 * k_2) = \phi(k_1) \circ \phi(k_2) = \bar{e}$.

$\therefore k_1 * k_2 \in K$.

Inverse

Let $k_1 \in K$.

~~$\phi(k_1 * k_1^{-1}) = \phi(e) = \bar{e} = \phi(k_1) \circ \phi(k_1^{-1})$~~

$\phi(k_1) = \bar{e}$.

$\phi(k_1^{-1}) = [\phi(k_1)]^{-1} = (\bar{e})^{-1} = \bar{e}$.

$\therefore k_1^{-1} \in K$.

Now normal subgroup.

Let $g \in G$.

$\therefore \phi(g k_1 g^{-1}) = \phi(g) \circ \phi(k_1) \circ \phi(g^{-1})$.

$= \phi(g) \circ \bar{e} \circ \phi(g^{-1})$

$= \phi(g) \circ [\phi(g)]^{-1}$

$= \bar{e}$

$\therefore \phi(g k_1 g^{-1}) = \bar{e}$

$\therefore g k_1 g^{-1} \in K \quad \forall\ g \in G, k_1 \in K$.

__/__/____

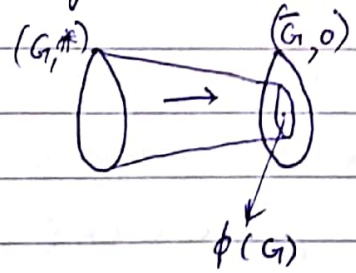
9) Suppose G is a group, N is a normal subgroup of G, define a mapping ϕ from G to G/N by $\phi(x) = Nx \ \forall x \in G$. Then show that ϕ is a homomorphism.

Let $x, y \in G$.

$$\phi(x * y) = N(x * y) = N^2(x * y)$$
$$= Nx \cdot Ny = \phi(x) \cdot \phi(y)$$

17/8/18.

Image set.



$$\phi(G) = \{\phi(x) \in \bar{G} \mid x \in G\}.$$

If $\phi(G) = \bar{G}$, it is an onto mapping $\Rightarrow$ surjective.

$\therefore$ Ker ϕ (kernel set) and $\phi(G)$ (image set) are of importance.

Let ϕ be a homomorphism from the group $(G, *)$ to $(\bar{G}, o)$. Show that $(\phi(G), o)$ forms a subgroup of $(\bar{G}, o)$.

$\phi(G) \subset \bar{G}$.

∴ We need to prove closure & inverse.

Closure

Let $x, y \in \phi(G)$.

∴ $\left.\begin{aligned} x &= \phi(a) \\ y &= \phi(b) \end{aligned}\right\}$ for some $a, b \in G$.

∴ $x \circ y = \phi(a) \circ \phi(b)$

$= \phi(a * b)$ [∵ homomorphism].

$= \phi(c)$ for $c \in G$. (G is closed).

∴ $x \circ y \in \phi(G)$.

∴ Closed.

Inverse

Let $x \in \phi(G)$.

∴ $x \circ x^{-1} = \bar{e}$

or, $\phi(a) \circ b = \bar{e}$

∴ $x^{-1} = [\phi(a)]^{-1}$

or, $\phi(a) \circ x^{-1} = \phi(a * a^{-1}) \Rightarrow x^{-1} = \phi(a^{-1})$.

Let $x \in G$

$x * x^{-1} = e$

$\phi(x * x^{-1}) = \phi(e)$

$\phi(x) \circ \phi(x^{-1}) = \bar{e}$

Also, $\phi(x) \circ [\phi(x)]^{-1} = \bar{e}$.

∴ $[\phi(x)]^{-1} = \phi(x^{-1})$

__/__/____

Since $x^{-1} \in G$, $\phi(x^{-1}) \in \phi(G) \Rightarrow \phi(x)^{-1}$ exists & $\in \phi(G)$.

$\therefore$ Inverse exists.

(Proved).

A homomorphism ϕ from G to $\bar{G}$ is said to be an isomorphism if ϕ is bijective.

G and $\bar{G}$ (two groups) are said to be isomorphic to each other if there exists an isomorphism between them, denoted by $G \cong \bar{G}$.

Show that

i) $G \cong G$ (Reflexive)

ii) If $G \cong \bar{G}$, then $\bar{G} \cong G$. (Symmetric)

iii) If $G \cong \bar{G}$, $\bar{G} \cong G^*$, then $G \cong G^*$ (Transitive)

__/__/____

Ring.

$(R, +, \circ)$ — $\circ$ → Multiplication; $+$ → Addition

Properties :-

1) Closure wrt $+$

$a+b \in R \quad \forall\, a, b \in R.$

2) ~~Associative~~ wrt $+$.

$a + (b+c) = (a+b) + c \quad \forall\, a, b, c \in R.$

3) Commutative wrt $+$.

$a+b = b+a \quad \forall\, a, b \in R.$

4) Zero Element (Identity wrt $+$)

$\exists$ Element 0 in R s.t., $a+0 = 0+a = a$

5) Additive Inverse

$\exists$ an element $(-a)$ st $a + (-a) = (-a) + a = 0$

6) Closure wrt $\circ$.

$a \circ b \in R \quad \forall\, a, b \in R.$

__/__/____

7. Associative wrt $\circ$

$a \circ (b \circ c) = (a \circ b) \circ c \quad \forall\ a, b, c \in R$.

8. Distributive

$a \circ (b+c) = a \circ b + a \circ c$ (Left Distributive)

$(b+c) \circ a = b \circ a + c \circ a$ (Right Distributive).

$(R, +, \circ)$ is a ring

$\Rightarrow$ 1) $(R, +)$ is an abelian group.

2) $(R, \circ)$ is a semi-group.

3) Distributive

If $a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$, then 1 is the unit element of the Ring. [Doesn't necessarily exist].

Q) Examples of

1) Ring with a unit element $\rightarrow (\mathbb{Z}, +, \cdot)$

2) Ring without a unit element $\rightarrow (E, +, \circ)$

E ↓ Even Integers.

Q) If R is a ring, then show that for all $a, b \in R$,

1. $a \cdot 0 = 0 \cdot a = 0$.
2. $a \cdot (-b) = (-a) \cdot b = -(ab)$.
3. $(-a) \cdot (-b) = ab$.

If $(R, +, \cdot)$ has an unit element 1, then

4) $(-1) \cdot a = -a$

5) $(-1) \cdot (-1) = 1$.

Ans) 1) Let $a \in R$

$\therefore a + 0 = 0 + a = a$.

$a \cdot (a + 0) = a \cdot a + a \cdot 0$

or, $a \cdot a = a \cdot a + a \cdot 0$ $[\because a + 0 = a]$

or, $\boxed{a \cdot 0 = 0}$

Similarly, $(a + 0) \cdot a = a \cdot a + 0 \cdot a$

or, $a \cdot a = a \cdot a + 0 \cdot a$ $[\because a + 0 = a]$

or, $\boxed{0 \cdot a = 0}$

$\therefore \boxed{a \cdot 0 = 0 \cdot a = 0}$

2) $a \cdot b + a \cdot (-b) = a \cdot (b + (-b))$

$= a \cdot 0$

$= 0$

or, $\boxed{a \cdot (-b) = -(a \cdot b)}$

Similarly, $(-a) \cdot b + a \cdot b = 0$

$\therefore \boxed{(-a) \cdot b = -(a \cdot b)}$

__/__/____

3) $(-a)\cdot(-b) = -(a\cdot(-b))$ [By $(-a)\cdot b = -(a\cdot b)$]

$= -(-(a\cdot b))$ [By $a\cdot(-b) = -(a\cdot b)$]

$= (a\cdot b)$.

4) Suppose R has a unit element 1 then

$a + (-1)\cdot a = 1\cdot a + (-1)\cdot a$

$= (1 + (-1))\cdot a$.

$= 0\cdot a$

$= 0$.

Also, $(-1)\cdot a + a = 0$.

$\therefore$ $(-1)\cdot a$ is additive inverse of a

$\therefore$ $(-1)\cdot a = -a$

5) If you take $a = -1$ in (4),

$(-1)\cdot(-1) = -(-1)$

$= 1$.

__/__/____

q) Let $(R, +, \cdot)$ be a Ring with unit element 1 s.t. $R \neq \{0\}$. Show that 0 and 1 are distinct elements.

Let $a \in R$.
Then, $a \cdot 0 = 0$
while $a \cdot 1 = a$
$\therefore$ 0 & 1 are distinct elements.

OR

Assume $0 = 1$
$a = a \cdot 1 = a \cdot 0 = 0 \neq a$
$\forall a \in R$
Since $R \in \{0\}$
contradiction.

$a \cdot 0 \neq a \cdot 1$
left cancellation
$0 \neq 1$

q) Let $(G, *)$ be an arbitrary commutative group and Hom_G be the set of all homomorphisms from $(G, *)$ onto itself. Then show that $(\text{Hom}_G, +, \circ)$ forms a ring with ~~Identity~~ unit element.

$+ \rightarrow (f+g)(a) = f(a) * g(a)$, $a \in G$
$\forall f, g \in \text{Hom}_G$.

$\circ \rightarrow$ functional composition.

Ans) 1) Closure wrt $+$.
Let $f, g \in \text{Hom}_G$, $a \in G$.
$(f+g)(a) = f(a) * g(a) \in G$.

$\therefore (f+g)$ maps a to $(f(a) * g(a)) \in G$.
$\therefore f+g \in \text{Hom}_G$.

22/8/18

Vector Space.

Till now Groups & Rings had just 1 set of elements.
Vector has 2 sets : $(V, \oplus)$ $(F, +, \cdot)$ $\oplus$: Vector addn.

$(F, +, \cdot)$ (of scalars)
F is a field $\Rightarrow$ It is a commutative division ring.
[Division Ring : Non zero elements form a group].
$(F - \{0\}, \cdot)$ forms a commutative group.
V forms a commutative group wrt vector addn.
F. . . . . scalar . . .
Here, there'll be operations between elements from 2 different sets for the 1st time (Eg. $2A + 3B$ where A : matrix)
↳ Scalar Mult.

$M_{2\times 2}$	$2A + 3B$
$\mathbb{R}^2$	$2(x,y) + 3(u,v)$
V	$2\vec{u} + 3\vec{v}$.

$(F, +, \cdot)$
Let F be a given field whose elements are called as scalars.
The set V is a non-void set whose elements are called as vectors.

The set $(V, \oplus)$ is a vector space over the field F if the following axioms are satisfied.

For any 2 vectors, $\bar{\alpha}, \bar{\beta} \in V$ $\quad \bar{\alpha} \oplus \bar{\beta} \in V$ (Closure)
$\bar{\alpha} \oplus \bar{\beta} = \bar{\beta} \oplus \bar{\alpha}$. (Commutativity)

(V3) (Associative)
For any three vectors, $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in V$, $\bar{\alpha} \oplus (\bar{\beta} \oplus \bar{\gamma}) = (\bar{\alpha} \oplus \bar{\beta}) \oplus \bar{\gamma}$.

(V4) $\exists$ unique vector $\bar{\phi} \in V$, such that

$\bar{\alpha} \oplus \bar{\phi} = \bar{\phi} \oplus \bar{\alpha} = \bar{\alpha} \quad \forall \ \bar{\alpha} \in V$. (Identity)

(V5) For any vector $\bar{\alpha} \in V$, $\exists$ a vector $-\bar{\alpha} \in V$, s.t.

$\bar{\alpha} \oplus (-\bar{\alpha}) = \bar{\phi} = (-\bar{\alpha}) \oplus \bar{\alpha}$. (Inverse)

5 more properties for $(F, +)$: Commutative Group
$(F - \{0\}, \cdot)$: ------

Now, for V with F,

(V6) For any element $a \in F$ and any vector $\bar{\alpha} \in V$,

$a\bar{\alpha} \in V$.

↳ Scalar Multiplication (Not '.' : within scalars).

(V7) For any element $a \in F$ and any vector $\bar{\alpha}, \bar{\beta} \in V$,

$a(\bar{\alpha} \oplus \bar{\beta}) = a\bar{\alpha} \oplus a\bar{\beta}$.

(V8) For any two scalars $a, b \in F$ and any vector $\bar{\alpha} \in V$,

$(a+b)\bar{\alpha} = a\bar{\alpha} \oplus b\bar{\alpha}$.

(V9) For any two scalars $a, b \in F$ and any vector $\bar{\alpha} \in V$,

$(a.b)\bar{\alpha} = a(b\bar{\alpha})$

(V10) For the unit scalar $1 \in F$ and any vector $\bar{\alpha} \in V$,

$1\bar{\alpha} = \bar{\alpha}$.

__/__/____

V1 – V5 : Internal Operations.
V6 – V10 : External Operations.

If V is vector space over the field F, it is denoted by V(F).
If F is Real Numbers $\mathbb{R}$, V(F) is called Real Vector space
.... Complex .. $\mathbb{C}$, ... Complex .....

Q) If V(F) is a vector space and $\bar{\alpha}, \bar{\beta}, \bar{\phi} \in V$ and $0, a, b \in F$, then show that :

(i) $a\bar{\phi} = \bar{\phi}$ (ii) $0\bar{\alpha} = \bar{\phi}$ (iii) $a(-\bar{\alpha}) = -(a\bar{\alpha})$
(iv) $(-a)\bar{\alpha} = -(a\bar{\alpha})$ (v) $a(\bar{\alpha} \oplus (-\bar{\beta})) = a\bar{\alpha} \oplus (-a\bar{\beta})$
(vi) $a\bar{\alpha} = \bar{\phi} \Rightarrow a = 0$ or $\bar{\alpha} = \bar{\phi}$.
(vii) $a\bar{\alpha} = b\bar{\alpha} \Rightarrow a = b$.
(viii) $a\bar{\alpha} = a\bar{\beta} \Rightarrow \bar{\alpha} = \bar{\beta}$.

Ans (i) $a \in F$, $\bar{\phi} \in V$ ($\bar{\phi}$ → identity)

$\bar{\alpha} \oplus \bar{\phi} = \bar{\alpha}$

$\Rightarrow a(\bar{\alpha} \oplus \bar{\phi}) = a\bar{\alpha}$

$\Rightarrow a\bar{\alpha} \oplus a\bar{\phi} = a\bar{\alpha}$

$\therefore a\bar{\phi} = \bar{\phi}$ [Proved]

$a\bar{\phi} = a(\bar{\phi} \oplus \bar{\phi})$

$a\bar{\phi} \oplus \bar{\phi} = a\bar{\phi} \oplus a\bar{\phi}$

$\therefore a\bar{\phi} = \bar{\phi}$.

(ii) $0 \in F$, $\bar{\alpha}, \bar{\phi} \in V$

$0 + a = a$

$(0+a)\bar{\alpha} = a\bar{\alpha}$

$0\bar{\alpha} \oplus a\bar{\alpha} = a\bar{\alpha} \Rightarrow 0\bar{\alpha} = \bar{\phi}$ [Proved].

(iii) $\bar{\alpha} \oplus (-\bar{\alpha}) = \bar{\phi}$.

$a(\bar{\alpha} \oplus (-\bar{\alpha})) = a\bar{\phi}$

$a\bar{\alpha} \oplus a(-\bar{\alpha}) = \bar{\phi}$ (from ①)

Let $a\bar{\alpha}$ be $\bar{v}$,

$\therefore \bar{v} \oplus a(-\bar{\alpha}) = \bar{\phi} \Rightarrow a(-\bar{\alpha}) = -\bar{v}$

$\therefore a(-\bar{\alpha}) = -(a\bar{\alpha})$

(iv) $(a+(-a))\bar{\alpha} = 0\bar{\alpha}$

$a\bar{\alpha} \oplus (-a)\bar{\alpha} = \bar{\phi}$

$(-a)\bar{\alpha}$ is the inverse of $a\bar{\alpha} \Rightarrow$

~~Similar as above~~ $(-a)\bar{\alpha} = -(a\bar{\alpha})$.

$\boxed{(-a)\bar{\alpha} = a(-\bar{\alpha}) = -(a\bar{\alpha})}$

(v) $a(\bar{\alpha} \oplus (-\bar{\beta})) = a\bar{\alpha} \oplus a(-\bar{\beta})$

$= a\bar{\alpha} \oplus (-a\bar{\beta})$ [from (iii)].

(vi) $a\bar{\alpha} = \bar{\phi}$

$\Rightarrow a\bar{\alpha} = a\bar{\phi}$ or $a\bar{\alpha} = 0\bar{\alpha}$.

$\therefore \bar{\alpha} = \bar{\phi}$ or $a = 0$.

(vii) $a\bar{\alpha} = b\bar{\alpha}$

$\Rightarrow a\bar{\alpha} \oplus (-b\bar{\alpha}) = \bar{\phi}$

or, $(a + (-b))\alpha = \bar{\phi}$

or, $a + (-b) = 0 \Rightarrow \boxed{a = b}$.

__/__/____

(viii) $a\bar{\alpha} = a\bar{\beta} \Rightarrow a\bar{\alpha} \oplus (-a\bar{\beta}) = \bar{\phi}$.

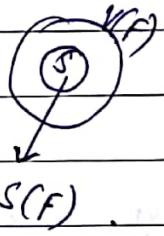
$(a\bar{\alpha} \oplus a(-\bar{\beta})) = \bar{\phi}$

$a(\bar{\alpha} \oplus (-\bar{\beta})) = \bar{\phi} \Rightarrow \bar{\alpha} \oplus (-\bar{\beta}) = \bar{\phi}$.

$\bar{\alpha} = \bar{\beta}$.

Subspace

A subset S of $V(F)$, would be a subspace $S(F)$ if :-



① $\bar{\alpha} \oplus \bar{\beta} \in S \quad \forall\ \bar{\alpha}, \bar{\beta} \in S$.

② $c\bar{\alpha} \in S \quad \forall\ \bar{\alpha} \in S, \forall\ c \in F$.

Additive inverse is not required to be proven explicitly, because scalar mult. with (-1) includes it.

$(-a)\bar{\alpha} = -(a\bar{\alpha}) =$ inverse of $a\bar{\alpha}$.

① $\Rightarrow$ S1 (V1 for set S).

S2, S3 are hereditary properties.

If $c = -1$, $c\bar{\alpha} = (-1)\bar{\alpha} = -(1\bar{\alpha}) = -\bar{\alpha} \in S$ (S5)

$\bar{\alpha} \in S, -\bar{\alpha} \in S \Rightarrow \bar{\alpha} \oplus (-\bar{\alpha}) \in S \Rightarrow \bar{\phi} \in S$ (S4).

② $\Rightarrow$ S6.

__/__/____

DIY S7-S10

Def^n subset of V
S is a subspace of V iff $a\bar{\alpha} \oplus b\bar{\beta} \in S$ $\forall \bar{\alpha}, \bar{\beta} \in S$, and $a, b \in F$.

① : $a = 1 \in$, $b = 1$ ② : $a = c$, $b = 0$

Q1) $V = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, x_i \in \mathbb{R} \right\}$. $(V, \oplus)$ is a vector space over $(\mathbb{R}, +, \cdot)$. $\oplus$: Matrix Addition.

Show that $S = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_2 & x_4 \end{bmatrix} \; x_i \in \mathbb{R} \right\}$ is a subspace of V

Q2) Let $\mathbb{R}^3 = \{(x_1, x_2, x_3) ; x_1, x_2, x_3 \in \mathbb{R}\}$

$(\mathbb{R}^3, \oplus)$ be a vector space over $(\mathbb{R}, +, \cdot)$

$\oplus \longrightarrow (x_1, x_2, x_3) \oplus (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$

Show that $S = \{(x_1, x_2, 0), x_i \in \mathbb{R}\}$ is a subspace of $\mathbb{R}^3$.