## Subgroup:

Let $(G,*)$ be a group and $H$ be a non-empty subset of $G$. If $(H,*)$ is a group where $*$ is an induced composition on $H$, then $(H,*)$ is a subgroup of $(G,*)$.

$(G,*)$ – ***Improper Subgroup*** of $(G,*)$

$(\{e\},*)$ – ***Trivial Subgroup*** of $(G,*)$

Any other subgroup is a ***Proper Subgroup*** of $(G,*)$.

**Example:** $(\mathbb{Z},+)$ is a proper subgroup of $(\mathbb{Q},+)$.

$(\mathbb{Q},+)$ is a proper subgroup of $(\mathbb{R},+)$.

Let $GL(2,\mathbb{R})$ denote the group of all $2\times 2$ real invertible matrices and let $SL(2,\mathbb{R})$ denote all $2\times 2$ real matrices with $|A|=1$; then $SL(2,\mathbb{R})$ is a subgroup of $GL(2,\mathbb{R})$.

## Result:

(1) Identity element of $(H,*)$ is the same as in $(G,*)$.

(2) The inverse of $a\in H$ in $(H,*)$ is same as in $(G,*)$.

(3) If $(G,*)$ is an abelian group then $(H,*)$ is also abelian.

All these results follow immediately from the fact that the binary composition has not changed from group to subgroup.

## Result:

A non-empty subset $H$ of a group $(G,*)$ will be a subgroup if and only if
(i) $a,b\in H\Rightarrow a*b\in H$ ; (ii) $a\in H\Rightarrow a^{-1}\in H$

If $(H,*)$ is a subgroup of $(G,*)\Rightarrow (H,*)$ is itself a group ⇒ both conditions are true [closure and existence of inverse].

Conversely if the conditions are true, then (i) holds ⇒closure is true

Associativity is true [hereditary property]

(ii) holds ⇒ existence of inverse property is satisfied

Combining (i) and (ii), since, $a\in H\Rightarrow a^{-1}\in H\Rightarrow a*a^{-1}\in H\Rightarrow e\in H$[existence of identity]

## Result:

A non-empty subset $H$ of a group $(G,*)$ will be a subgroup if and only if $a,b\in H\Rightarrow a*b^{-1}\in H$.

If $(H,*)$ is a subgroup of $(G,*)\Rightarrow (H,*)$ is itself a group ⇒ condition is true [closure and existence of inverse].

Conversely, if the condition is true, then $a,a\in H\Rightarrow a*a^{-1}\in H\Rightarrow e\in H$ [Identity]

Associativity is true [**Hereditary property:** as it is true in $G$, it is also true in $H$]

Using the condition, $e,a\in H\Rightarrow a^{-1}\in H$ [Inverse]

Also using the condition, $a,b^{-1}\in H\Rightarrow a*(b^{-1})^{-1}\in H\Rightarrow a*b\in H$ [Closure].

## Result:

$(G,*)$ be a group and $H, K$ be subgroups of $G$. Then $H \cap K$ is a subgroup of $G$.

$H \cap K \neq \phi, [\because e \in H \; and \; e \in K]$

Let $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$a, b \in H \Rightarrow a * b^{-1} \in H$ [$\because (H,*)$ is a subgroup of $(G,*)$] ;

$a, b \in K \Rightarrow a * b^{-1} \in K$ [$\because (K,*)$ is a subgroup of $(G,*)$]

Hence, $a * b^{-1} \in H \cap K \Rightarrow H \cap K$ is a subgroup of $G$.

## Result:

$(G,*)$ be a group and $H, K$ be subgroups of $G$. Then $H \cup K$ is not necessarily a subgroup of $G$.

Let $(G,*) = (\mathbb{Z}, +)$, and $(H,*) = (2\mathbb{Z}, +), (K,*) = (3\mathbb{Z}, +)$

Then, $2 \in H \cup K$, $3 \in H \cup K$, but, $2 + 3 = 5 \notin H \cup K$.

## Cyclic Group:

A group $(G,*)$ is said to be cyclic if there exists an element $a \in G$ such that, $G = \{a^n : n \in \mathbb{Z}\}$, denoted by, $G = \langle a \rangle$.

The element $a$ is called the generator of the cyclic group $G$.

Generator of a cyclic group is not unique.

In additive notation, $G = \langle a \rangle = \{na : n \in \mathbb{Z}\}$

**Example:** $(\mathbb{Z}, +) = \langle 1 \rangle$ ; also $(\mathbb{Z}, +) = \langle -1 \rangle$

**Example:** Klein's 4 group $\{e, a, b, c\}$ is not cyclic.

**Result:** If $G = \langle a \rangle$ then $a^{-1}$ is also a generator.

Since $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{(a^{-1})^{-n} : -n \in \mathbb{Z}\}$.

**Result:** If $G = \langle a \rangle$ then it is abelian.

If $x, y \in G \Rightarrow x = a^m; y = a^n, \; m, n \in \mathbb{Z} \Rightarrow x * y = a^m * a^n = a^{m+n} = a^{n+m} = y * x$

**Note:** Converse is not true as is the case with Klein's 4 group.

**Result:** If $G = \langle a \rangle$ is finite, then $o(G) = n \; iff \; o(a) = n$.

Let, $o(a) = n \Rightarrow \{a, a^2, \dots, a^n = e\} \subset G$ in which elements are all distinct.
(**Because**, **If not then** $\boldsymbol{a^p = a^q, p < q < n}$, $\boldsymbol{(say) \Rightarrow a^{q-p} = e}$, $\boldsymbol{q - p < n}$ **[contradiction])**

Also, $G = \{a^n : n \in \mathbb{Z}\}$

Let $x \in G \Rightarrow x = a^m = a^{qn+r} = a^r \in \{a, a^2, \dots, a^n = e\}$

Thus, $G = \{a, a^2, \dots, a^n\} \Rightarrow o(G) = n$.

Conversely, if $o(G) = n$, then if $o(a) = k$ (say), then by the previous argument $o(G) = k$.

A contradiction, implying that $o(a) = n$.

**Result:** $G$ is a finite cyclic group of order $n\ iff$ it has an element of order $n$.

If $G = \langle a \rangle \Rightarrow o(a) = o(G) = n$; then $\exists a \in G$ such that $o(a) = n$

Conversely, Let, $o(b) = o(G) = n$ ; we have to show that $G$ is cyclic.

Now, $o(b) = n \Rightarrow b, b^2, \dots, b^n = e$ are all distinct elements of $G$.

Hence, $G = \{b, b^2, \dots, b^n = e\}$, as $o(G) = n \Rightarrow G \subset \{b^n : n \in \mathbb{Z}\} \dots (1)$

Again since, $b \in G \Rightarrow b^n \in G$ , $\forall n \in \mathbb{Z}$ [closure]$\Rightarrow \{b^n : n \in \mathbb{Z}\} \subset G \dots (2)$

Combining $(1)\&\ (2)$ shows that $G$ is cyclic generated by $b$.

**Corollary:** if $G = \langle a \rangle$ ; then $G$ is infinite $iff$ $o(a)$ is infinite.

Let $o(a)$ is infinite. Then $a, a^2, a^3, \dots$ are all distinct elements of $G$;

otherwise if $a^m = a^n \Rightarrow a^{m-n} = e$ [contradiction]$\Rightarrow G$ is infinite.

Conversely, if $G$ is infinite then $o(a)$ is infinite, otherwise if $o(a) = n \Rightarrow o(G) = n$ [**Contradiction**, since $G$ is infinite]

**Result:** Let $G = \langle a \rangle$ is of order $n$. Then $a^k$ is a generator $iff \gcd(k, n) = 1$.

order of a cyclic group $\Leftrightarrow$ order of its generator $\Leftrightarrow o(a^k) = n$

Now we know that if $o(a) = n$, then, $o(a^k) = \frac{n}{\gcd(k,n)}$

Since $o(a) = n \Leftrightarrow o(a^k) = \frac{n}{\gcd\,(k,n)} = n \Leftrightarrow \gcd(k, n) = 1$.

**Result:** Every subgroup of a cyclic group is cyclic.

Let $G$ be cyclic and $H$ be its subgroup. If $H = \{e\}$, it is cyclic. Let $H \neq \{e\} \Rightarrow h \neq e \in H$.

$h = a^p,\ p \in \mathbb{Z} \Rightarrow a^{-p} \in H \Rightarrow \exists$ some positive integral powers of $a$ in $H$.

Let, $m$ be the least positive integer, s.t. $a^m \in H$ $[well - ordering\ principle\ of\ \mathbb{N}]$.

Then, $h = a^p = a^{mq+r}, 0 \leq r < m$

Now, $a^p \in H\ \&\ a^m \in H \Rightarrow (a^m)^q \in H \Rightarrow a^{mq} \in H \Rightarrow a^{p-mq} \in H \Rightarrow a^r \in H$

This is a contradiction as, $\boldsymbol{m}$ **is the least positive number s.t.** $\boldsymbol{a^m \in H}$, $\&\ \boldsymbol{r < m}$

This means that $r = 0 \Rightarrow p = mq \Rightarrow h = (a^m)^q \Rightarrow H = \langle a^m \rangle$.

**Result:** Let $G = \langle a \rangle$ is of order $n$. If $d$ is a positive divisor of $n$, then there exists a unique subgroup of $G$ of order $d$.

Let, $n = kd,\ k \in \mathbb{N}$;

Let us consider $\langle a^k \rangle$, the cyclic subgroup generated by, $a^k = b,\ (say)$

Now, $b^d = a^{kd} = e$; let $o(b) = m \Rightarrow m | d \dots (1)$

also, $b^m = e \Rightarrow a^{km} = e \Rightarrow n | km \Rightarrow d | m \dots (2) \Rightarrow m = d = o(a^k) \Rightarrow o(\langle a^k \rangle) = d$.

<u>Uniqueness:</u> let $o(\langle a^r \rangle) = d \Rightarrow a^{rd} = e \Rightarrow n | rd \Rightarrow k | r \Rightarrow a^r \in \langle a^k \rangle$.

Also, $o(a^r) = d = o(\langle a^k \rangle) \Rightarrow a^r$ is a generator of $\langle a^k \rangle \Rightarrow \langle a^r \rangle = \langle a^k \rangle$.

## Problems on Chapter 2:

1. $(G,*)$ is a group and $H$ is a non-empty finite subset of $G$. Then $(H,*)$ is a subgroup of $(G,*)$ if and only if $a, b \in H \Rightarrow a * b \in H$.

2. If $G = GL(2,\mathbb{R})$ and $H = \{A \in G : \det(A) = 1\}$. Examine if $H$ is a subgroup of $G$.

3. $(G,\circ)$ and $(H,*)$ be two groups. Define $\odot$ on $G \times H$ as $(g,h) \odot (g',h') = (g \circ g', h * h')$. Prove that $(G \times H,\odot)$ is a group. (External Direct Product of groups)

4. Show that the group $(\{1,2,3,4,5,6\},\times_7)$ is cyclic. Find the generators.

5. Show that $(\mathbb{Q},+)$ is non-cyclic and hence deduce that $(\mathbb{R},+)$ is also non-cyclic.

6. Examine if $(S,.)$, $S = \{z \in \mathbb{C} : z^n = 1\}$, is cyclic.

7. Find all generators of a cyclic group of order 10.

8. If $G$ is a group such that $(ab)^m = a^m b^m$ for three consecutive integers $m$, and $\forall a, b \in G$, show that $G$ is abelian.

9. Show that in a group $G$, for any two elements $a, x \in G$, $o(x^{-1}ax) = o(a)$.

Hints & Solutions:

1. Since H is non-empty, let $a \in H \Rightarrow a, a^2, a^3, \ldots \in H$;
   Since H is finite then we must have $a^i = a^j; i > j \Rightarrow a^{i-j} = e; i - j \geq 1$; hence $e \in H$
   Also, $i - j - 1 \geq 0; (a^{i-j-1}).a = a^{i-j} = e;\ i.e.\ a^{i-j-1} \in H$ is the inverse of $a$.

2. Clearly $H$ is non-empty as $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ let $A, B \in H$, then $|A| = |B| = 1$
   Then, $|AB| = |A||B| = 1$; Hence $AB \in H$ ; also, $|A^{-1}| = \frac{1}{|A|} = 1$; Hence, $A^{-1} \in H$.
   Hence, using the subgroup test, we can say that $H$ is a subgroup of $GL(2,\mathbb{R})$.

   **Note:**
   **$H$ is called the $SL(2,\mathbb{R})$ [Special Linear Group] a subgroup of $GL(2,\mathbb{R})$ [General Linear Group]**

3. Closure is obvious;
   [Associative]: $(g,h) \odot \{(g_1,h_1) \odot (g_2,h_2)\} = (g \circ g_1 \circ g_2, h * h_1 * h_2) = \{(g,h) \odot (g_1,h_1)\} \odot (g_2,h_2)$
   [Identity] : $(e_g,e_h)$ as, $(g,h) \odot (e_g,e_h) = (g \circ e_g, h * e_h) = (g,h)$;
   [Inverse] : $(g,h)$ is $(g^{-1},h^{-1})$, as, $(g^{-1},h^{-1}) \odot (g,h) = (g^{-1} \circ g, h^{-1} * h) = (e_g,e_h)$
   Hence, $G \times H$ forms a group under the given binary composition $\odot$.

   ***Note:***
   **If $G_1, G_2, \ldots, G_n$ be $n$ number of groups then their external direct product (E.D.P.) is defined as $(G_1 \times G_2 \times \ldots \times G_n,\odot)$ as $(g_1, g_2, \ldots, g_n) \odot (h_1, h_2, \ldots, h_n) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2, \ldots, g_n \circ_n h_n)$**

4. Consider 3; since $3^6 = 1(mod\ 7) \Rightarrow o(3) = 6 = o(G) \Rightarrow G = \langle 3\rangle$;
   Again, $3^{-1} = 5$ [$\because 3 \times 5 = 15 = 1\ (mod\ 7)$]; hence $G = \langle 5\rangle$; hence generators are 3,5.

5. First, let us assume that $(\mathbb{Q}, +)$ is cyclic.
   let, $(\mathbb{Q}, +) = \langle a\rangle = \{na : n \in \mathbb{Z}\}$;
   Now, $\frac{1}{2}a \in \mathbb{Q}$ , which cannot be written as $na : n \in \mathbb{Z} \Rightarrow (\mathbb{Q}, +)$ is not cyclic.
   We know that, every subgroup of a cyclic group is cyclic.
   Now If $(\mathbb{R}, +)$ is cyclic then so is $(\mathbb{Q}, +)$ as $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$ ; which is a contradiction as it is already proved that $(\mathbb{Q}, +)$ is not cyclic. Hence $(\mathbb{R}, +)$ is also non-cyclic.

6. Let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in S$,
   Now, $\omega^n = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^n = \cos 2\pi + i\sin 2\pi = 1 \Rightarrow\ o(\omega) = n = o(S) \Rightarrow S = \langle\omega\rangle$
   Thus, $S$ is cyclic.

7. Let $G = \langle a\rangle \Rightarrow o(a) = 10$;
   Now, $a^k$ is also a generator if $\gcd(k, 10) = 1 \Rightarrow k = 1,3,7,9$
   Hence, $G = \langle a\rangle, \langle a^3\rangle, \langle a^7\rangle, \langle a^9\rangle$
   In all there are 4 generators for this group.

8. Let, the result be true for three consecutive integers $m, m+1, m+2$; then,
   $(ab)^m = a^m b^m$, $(ab)^{m+1} = a^{m+1}b^{m+1}$ and $(ab)^{m+2} = a^{m+2}b^{m+2}$
   Hence, $(ab)^{m+2} = a^{m+2}b^{m+2} \Rightarrow (ab)^{m+1}.ab = a.a^{m+1}.b^{m+1}.b$
   substituting the value of $(ab)^{m+1}$ in L.H.S. as $a^{m+1}.b^{m+1}$ we get,
   giving, $a^{m+1}.b^{m+1}.ab = a.a^{m+1}.b^{m+1}.b \Rightarrow a.a^m.b^m.b.a.b = a.a^{m+1}.b^{m+1}.b$
   By left and right cancellation, we get, $a^m.b^m.b.a = a^{m+1}.b^{m+1}$
   Using the results, we have, $(ab)^m.ba = (ab)^{m+1} = (ab)^m.ab \Rightarrow ba = ab$
   Hence the group is abelian.

9. Let $o(a) = n$ ;
   Then, $(x^{-1}ax)^n = (x^{-1}ax).(x^{-1}ax) \ldots\ldots (x^{-1}ax)$
   $= x^{-1}a^n x = e$
   This implies that $o(x^{-1}ax)\ is\ finite,\ say\ m \Rightarrow m|n \ldots (1)$
   $Again,\ (x^{-1}ax)^m = e \Rightarrow x^{-1}a^m x = e \Rightarrow a^m = e \Rightarrow n|m \ldots (2)$;
   $combining\ (1)\&\ (2), we\ get,\ n = m.$

Assignments on Chapter 2:

1. $(G,*)$ is an abelian group and $H$ is a subgroup of $G$. Let $K = \{x \in G : x^2 \in H\}$. Examine if $(K,*)$ is a subgroup of $(G,*)$.

2. Let $a, b$ be two fixed integers and $H = \{ax + by : x, y \in \mathbb{Z}\}$. Examine if $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$.

3. Examine if $(\mathbb{Z}_5, +_5)$ is a cyclic group and if so, find its generators.

4. Prove that an infinite cyclic group can have only two generators.

5. If $G$ is a group such that $a^2 = e$ , $\forall a \in G$, show that $G$ is abelian.

6. Show that a group with 4 elements is necessarily abelian.