IMPORTANT DEFINITIONS AND EXAMPLES

Definition

A subset H of a group G is called a **subgroup** of G if H forms a group with respect to the binary operation in G.

Example.1

Let G be any group.
Then $\{e\}$ and G are subgroups of G and this subgroups are called **Improper subgroups** of G.

Example.2

$(Q, +)$ is a subgroup of $(R, +)$ and $(R, +)$ is a subgroup of $(C, +)$.

Example.3

$\{1, -1, i, -i\}$ is a subgroup of $(C^*, .)$.

Example.4

In $(Z_8, \oplus)$ $H_1 = \{0, 4\}$ and $H_2 = \{0, 2, 4, 6\}$ are subgroups of $(Z_8, \oplus)$.

Definition

Let G be a group.
Then the subgroup $H = \{a/a \in Gandax = xaforallx \in G\}$ is called the **centre of** G and is denoted by $Z(G)$.

Definition

Let G be a group and let a be a fixed element of G.
Then the subgroup $H_a = \{x\ x \in Gandax = xa\}$ is called the **Normaliser of** a **in** G.

Definition

Let G be a group.
Let $a \in G$. Then the subgroup $H = \{a^n / n \in Z\}$ is called the **cyclic subgroup of G generated by** a and is denoted by $< a >$.

Definition

A group G is **cyclic** if there exists a an element $a \in G$ such that $G =< a >$.

Example.5

In $(Z,+), <2>= 2Z$ is a cyclic subgroup of Z.

Example.6

The group $G = \{1, -1, i, -i\}$ is cyclic group generated by $< i >$ and $< -i >$.

Example.7

$(Z_8, \oplus)$ is a cyclic group generated by 1,2,5 and 7.

Example.8

$(nZ, +)$ is a cyclic group generated by n and $-n$.

Example.9

The group $G = \{1, \omega, \omega^2\}$ is a cyclic group generated by ω and ω^2.

Example.10

$(R,+)$ is not a cyclic group, since for any $x \in R, < x >= \{nx/n \in Z\} \neq R$.

Definition

Let G be a group. Let $a \in G$. Then **Order of a O(a)** is the least positive integer n (if it exists) such that
$a^n = e$.
If there is no positive integer n such that $a^n = e$ then **O(a)** is infinite.

Example.11

In any group G, e is the only element of order 1.

Example.12

In the group $G\{1, -1, i, -i\}$, o(1)=1, o(-1) = 2, o(i)=4, o(-i)=4.

Example.13

In $(Z_8, \oplus)$ o(2)=4 and o(3)=8.

Definition

Let H be a subgroup of G.
Let $a \in G$.
Then the set $aH = \{ah/h \in H\}$ is called the **Left Coset of H defined by a in G**
Similarly, $Ha = \{ha/h \in H\}$ is called **Right Coset of H defined by a in G**

Example.14

Let $G = (Z_{12}, \oplus)$.
Then $H = \{0, 4, 8\}$ is a subgroup of G.
The left cosets of H are
$0 + H = \{0, 4, 8\} = H$
$1 + H = \{1, 5, 9\}$
$2 + H = \{2, 6, 10\}$
$3 + H = \{3, 7, 8\}$
Note that $4 + H = \{0, 4, 8\} = H$ and $5 + H = \{5, 9, 1\} = 1 + H$ etc..

Definition

Let H be a subgroup of G. Then the number of distinct left(right) cosets of H in G is called the **Index of H in G**
and is denoted by $[G : H]$

Example.15

Let $G = (Z_8, \oplus)$.
Then $H = \{0, 4, \}$ is a subgroup of G.
The left cosets of H are
$0 + H = \{0, 4\} = H$
$1 + H = \{1, 5\}$
$2 + H = \{2, 6\}$
$3 + H = \{3, 7\}$
There are four distinct left cosets of H in G.
Thus $[G : H] = 4$

Important Theorems

Theorem.1

Let H be a subgroup of G. Then
(i) The identity element of H is same as that of G.
(ii). For each $a \in H$ the inverse of a in H is same as the inverse of a in G.

Proof.

(i). Let e and e' be the identities of G and H respectively.
Let $a \in H$. Then, $e'a = a$(since e' is the identity of$H$).
Now,$a = ea$(since e is the identity of$G$ and $a \in G$).
Therefore $e'a = ea$
Thus $e' = e$ (By right cancellation law). Hence (i).
(ii). Let a' be the inverse of a in G.
Let a'' be the inverse of a in H.
Then $a.a' = e = a.a''$.
Hence by Cancellation law, we have $a' = a$". Hence (ii).

Theorem.2

A subset H of a group G is a subgroup of G iff
(i). it is closed under the binary operation in G.
(ii). The identity e of G is in H.
(iii). $a \in H \Rrightarrow a^{-1} \in H$.

Proof.

Let H be a subgroup of G. Then By theorem 1, we have (i),(ii) and (iii).
Conversely let H be a subset of G satisfying conditions (i), (ii) and (iii).
Then, clearly H itself a group under the same binary operation in G.
Hence H is a subgroup of G.

Theorem.3

A non-empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof.

Let H be a subgroup of G.
Let $a, b \in H$.
Since H is subgroup, $b \in H \Rightarrow b^{-1} \in H$
Thus $a, b^{-1} \in H \Rightarrow ab^{-1} \in H$ (by Closure law).
Conversely, Let H be a non empty subset of G such that
$a, b \in H \Rightarrow ab^{-1} \in H$......(1)
We have to prove that H is a subgroup of G.

Since H is non-empty, there exists an element $a \in H$.
Hence $aa^{-1} \in H$ (by (1).
Thus $e \in H$.
Now $e, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$.
Let $a, b \in H$.
Then $a, b^{-1} \in H$.
By (1), $a(b^{-1})^{-1} \in H$.
i.e $ab \in H$. Hence H is closed under the binary operation in G.
Thus By Theorem 2, H is a subgroup of G.

Theorem.4

Let H be a non-empty finite subset of G.
If H is closed under the binary operation in G then H is subgroup of G.

Proof.

Let $a \in H$. Since H is closed and finite, $a, a^2, a^3, ...a^n, ...$ are all elements of H
and cannot all be distinct.
Let $a^r = a^s, r < s$.
Then $a^{s-r} = e \in H$.
Let $a \in H$.
We have proved for some $n, a^n = e$.
Hence $aa^{n-1} = e$.
Thus $a^{-1} = a^{n-1}$.
Hence H is a subgroup of G.

Remark.

The converse of above theorem is not true if H is finite.

Proof.

We know that N is subset of $(Z, +)$.
Also N is closed under addition.
But N is not a subgroup of $(Z, +)$.

Theorem.5

The intersection of any two subgroups of group G is also a subgroup of G.

Proof.

Let H and G be two subgroups of G.
Then $e \in H$ and $e \in K$. Thus $e \in H \bigcap K$.
Hence $H \bigcap K$ is non-empty subset of G.
Now, let $a, b \in H \bigcap K$. Then $a, b \in H$ and $a, b \in K$.
Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$.
Thus $ab^{-1} \in H \bigcap K$.
Hence $H \bigcap K$ is subgroup of G.

Theorem. 6

The union of two subgroups of group G is a subgroup if and only if one is contained the other.

Proof.

Let H and G be two subgroups of G such that one is contained the other.

i.e., Either $H \subseteq K$ or $K \subseteq H$.

Thus $H \bigcup K = K$ or $H \bigcup K = H$.

Hence $H \bigcup K$ is a subgroup of G.

Conversely, let us assume that $H \bigcup K$ is subgroup of G.

We have to prove that $H \subseteq K$ or $K \subseteq H$
Suppose that H is not contained in K and K is not contained in H.
Then there exist elements a, b such that $a \in H$ and $a \notin K$......(1)
and $b \in K$ and $b \notin H$......(2)
Clearly $a, b \in H \bigcup K$.Since $H \bigcup K$ is subgroup of G, $ab \in H \bigcup K$.
Hence $ab \in H$ or $ab \in K$.
Case(1). Let $ab \in H$. Since $a \in H$, we have $a^{-1} \in H$.
Thus $a^{-1}(ab) = b \in H$ which is contradiction to (2).
Case(2). Let $ab \in K$. Since $b \in K$, we have $b^{-1} \in K$.
Thus $(ab)b^{-1} = a \in K$ which is contradiction to (1).
Hence our assumption that H is not contained in K and K is not contained in H is wrong.
Thus, $H \subseteq K$ or $K \subseteq H$.

Theorem. 7

Let A and B be two subgroups of a group G.
Then AB is a subgroup of G if and only if $AB = BA$.

Proof.

Let AB be a subgroup of G.
We claim that $AB = BA$.
Let $x \in AB$.
Since AB is a subgroup of G, we have $x^{-1} \in AB$.
Let $x^{-1} = ab$ where $a \in A$ and $b \in B$.
Therefore, $x = (ab)^{-1} = b^{-1}a^{-1} \in BA$
Hence $AB \subseteq BA$.
Similarly we can prove $BA \subseteq AB$.
Thus $AB = BA$.

Conversely, Let $AB = BA$.
We have to prove that AB is a subgroup of G.
Clearly, $e \in AB$ and hence AB is non-empty.
Now, let $x, y \in AB$.
Then $x = a_1 b_1$ and $= a_2 b_2$ where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.
Now, $xy^{-1} = a_1 b_1 (a_2 b_2)^{-1} = a_1 b_1 b_2^{-1} a_2^{-1}$
$b_2^{-1} a_2^{-1} \in BA$.
Since $BA = AB$, $b_2^{-1} a_2^{-1} \in AB$.
$b_2^{-1} a_2^{-1} = a_3 b_3$ where $a_3 \in A$ and $b_3 \in B$.
Therefore, $xy^{-1} = a_1 b_1 a_3 b_3$
Now, $b_1 a_3 \in BA$. Since $BA = AB, b_1 a_3 \in AB$
Thus, $b_1 a_3 = a_4 b_4$, where $a_4 \in A$ and $b_4 \in B$.
Therefore $xy^{-1} = a_1 (a_4 b_4) b_3 \in AB$
Hence, AB is a subgroup of G.

Corollary. If A and B are subgroups of an abelian group G, then AB is a subgroup of G.

Proof. Let $x \in AB$.
Then $x = ab$ where $a \in A$ and $b \in B$.
Since G is abelian, $ab = ba$.
Therefore, $x \in BA$. Hence $AB \subseteq BA$.
Similarly $BA \subseteq AB$.
Thus $AB = BA$.
Hence AB is a subgroup of G.