Theorem 6: If H is any subgroup of G, then G is equal to the union of all right cosets of H in G.

Proof: To prove $G = \bigcup_{a \in G} Ha$. We show that

$\bigcup Ha \subseteq G$ and also $G \subseteq \bigcup Ha$.

Since each right coset is a subset of G, the union of all right cosets is a subset of G.

i.e. $$\bigcup_{a \in G} Ha \subseteq G \quad -(1)$$

for any $a \in G$,

$$a = ea \in Ha, \quad e \in H$$

$$a \in \bigcup_{a \in G} Ha$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} Ha \quad -(2)$$

$$G = \bigcup_{a \in G} Ha$$

Ex: $G = \{1, -1, i, -i\}$.

$1 \in G$

$G = H1 \cup Hi$

$H = \{1 \quad -1\}$ ✓

$H(i) = \{i \quad -i\}$

$H(-i) = \{-i \quad i\}$

$H1 = H$

$H(-1) = \{-1 \quad 1\} = H = H1$

Lagrange's Theorem:

Let G be a finite group and H be a subgroup of G. Then the order of H (i.e., no. of elements in H) divides the order of G.

Proof: Let $Ha_1, Ha_2, \ldots, Ha_k$ be all the right cosets of G.

We know $G = \bigcup_{i=1}^{k} Ha_i$

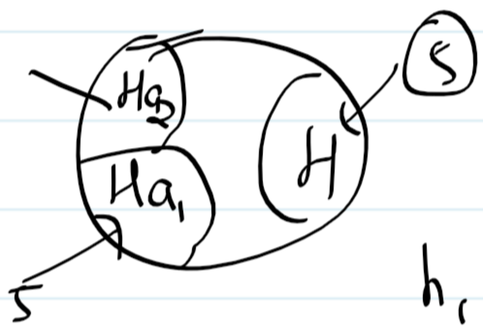
$= Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$

$= o(Ha_1) + o(Ha_2) + \cdots + o(Ha_k)$

$= o(H) + o(H) + \cdots + o(H)$

$o(G) = k \cdot o(H)$

$\Rightarrow o(H) \mid o(G)$



$h_1, h_2 \in H$

$Ha_1 = \{ h_1a_1, h_2a_1, h_3a_1 \}$

$h_i a_1 = h_j a_1 \Rightarrow h_i = h_j$

$\Rightarrow o(H) = o(Ha_1)$

Order of an element :

Let G be a group & $a \in G$. The smallest +ve integer n s.t. $a^n = e$, is called order of an element a & is denoted by $o(a)$.

Example : $G = \{1 \quad -1 \quad i \quad -i\}$ → multiplication.

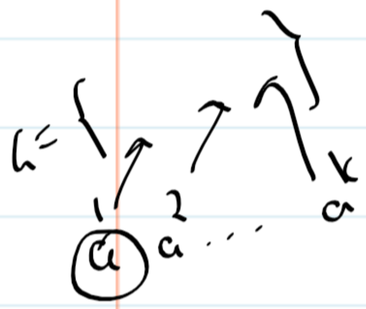
$e = 1$

$o(1) = 1$ as $1^1 = 1$

$o(i) = 4$ as $i^4 = 1$ $\quad i^1 = i$ $\quad i^2 = -1$ $\quad i^3 = -i$ $\quad i^4 = 1$

$o(-1) = 2$ as $(-1)^2 = 1$

$o(-i) = 4$ as $(-i)^4 = 1$



Cyclic group : A group G is said to be cyclic, if there exist an element $a \in G$ such that every element of G can be written as a power of a. Then 'a' is called the generator of a and denoted by $G = (a)$.

Example : $G = \{1 \quad -1 \quad i \quad -i\}$ w.r.to multiplication

Check whether $G = (i)$ or $G = (-i)$

$i^1 = i$ $\quad i^2 = -1$ $\quad i^3 = -i$ $\quad i^4 = 1$

$G = (i)$ i is the generator.

$-i$ is also a generator of G.

2) $G = \{1 \quad \omega \quad \omega^2\}$ w.r.to multiplication.

Is G a cyclic group? Yes

$G = (\omega)$ also $G = (\omega^2)$

Theorem 1 : A cyclic group is always abelian.

Proof : Let G be a cyclic group & let $G = (a)$.

Let $x, y \in G$ then $x = a^m$, $y = a^n$ for $m, n \in Z$.

$$x.y = a^m a^n = a^{m+n} = a^n a^m = yx$$

$\Rightarrow$ G is abelian.

Note : Converse need not be true.

$(Z, +)$ is abelian but not cyclic.

$Z : \{ \ldots -2 \ -1 \ 0 \ 1 \ 2 \ldots \}$

$(Z^+, +)$ is abelian & cyclic.

Theorem 2: Every groups of prime order is abelian.

Proof: We prove that a group with prime order is cyclic. Hence it is abelian.

Let $o(G) = p$, p is a prime number.

Then there is an element $a \in G$ s.t $a \neq e$

Consider the subset $H = (a) = \{ a^n \mid n \in \mathbb{Z} \}$

To prove H is a subgroup of G.

$x, y \in H$, will show $xy^{-1} \in H$

$x = a^m$, $y = a^n \Rightarrow xy^{-1} = a^m \cdot (a^n)^{-1}$

$a^n \in$ $a^{m-n} \in H$

$\Rightarrow H$ is subgroup & it is cyclic.

By Lagrange's Theorem $o(H) \mid o(G)$

$\Rightarrow o(H) = 1$ or $o(H) = p$

But $o(H) \neq 1$ as $a \neq e$

$\Rightarrow o(H) = p$

$\Rightarrow G = H \Rightarrow G = (a)$

As G is cyclic, G is abelian.

Problems :

1) Show that $Z_5 = \{0, 1, 2, 3, 4\}$ forms a cyclic group under the operation of addition modulo 5. List all the elements of Z_5 that generate it.

Soln :

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a \oplus_5 e = a$

$a \oplus_5 b = e$

$1 + 4 = 0$

e

$e = 0$

inverse of $0 \rightarrow 0$

$1 \rightarrow 4$

$2 \rightarrow 3$

$3 \rightarrow 2$

$4 \rightarrow 1$

$1 = 1 =$

$1^2 = 1 \oplus_5 1 = 2$

$1^3 = 1 \oplus_5 1 \oplus_5 1 = 3$

$1^4 = 4$

$1^5 = 0$

Its a group.

cyclic group

Generators are 1, 2, 3, 4.

2 is a generator :

$2^1 = 2$

$2^2 = 2 + 2 = 4$

$2^3 = 2 +_5 2 +_5 2 = 1$

$2^4 = 2 + 2 + 2 + 2 = 3$

$2^5 = 0$.

Z_6

$\{0 \quad 1 \cdots \quad 5\}$

2

2) Show that subgroup of a cyclic group is again cyclic.

Soln: Let $G = (a)$ be cyclic group. H be a subgroup

Elements of H are of the form a^n for $n \in Z$

Let s be the smallest $+^{ve}$ integer s.t $a^s \in H$.

We show that $H = (a^s)$. i.e H is a cyclic group with generator a^s.

Let $x \in H$, then $x = a^m$, $m \in Z$

But $m = qs + r$, $0 \leq r < s$

suppose $r \neq 0$

$x = a^m = (a^s)^q$

$r = m - qs$,

$a^r = a^{(m-qs)} = a^m (a^{qs})^{-1}$

$a^m \in H$, $a^{qs} \in H$, $(a^{qs})^{-1} \in H \Rightarrow a^r \in H$

Contradiction to the fact that s is smallest $0 \leq r < s$

$\Rightarrow r = 0$

$\Rightarrow m = qs$

$a^m = (a^s)^q$

$\Rightarrow x = (a^s)^q$

$\longrightarrow H = (a^s)$

H is a cyclic subgroup.

3) Show that order of an element divides the order of the group

Soln: Let $a \in G$ and n be the order of the element a, i.e, $a^n = e$, $o(a) = n$.

Let $H = (a) = \{ a^n \mid n \in Z \}$ be a cyclic group

$o(H)$ is atmost n.

Suppose $a^i = a^j$ $\quad 0 < i < j < n$

then $a^{i-j} = e$

$\Rightarrow$ Contradiction to the fact that $a^n = e$

$a^i \neq a^j$ for all $i \neq j$

$\Rightarrow o(H) = n$

By Lagrange theorem $\rightarrow$ $o(H) \mid o(G)$

$n \mid o(G)$

$o(a) \mid o(G)$

4) Let G be a group of finite order. Let $a \in G$. Then show that $a^{o(G)} = e$.

Soln: $o(a) \mid o(G)$

$$o(G) = q\, o(a)$$

$$a^{o(G)} = a^{q\,o(a)} = \left(a^{o(a)}\right)^q = e^q = e$$

5) If G is cyclic with generator a, show that $o(a) = o(G)$.

Soln: $G = (a) = \{ a \quad a^2, \ldots \quad a^n \}$ we know $a^n = e$

G has at most n elements.

Suppose $a^i = a^j$

$a^{i-j} = e$

Contradiction to our fact n is smallest.

$\longrightarrow$ G has n elements or G has $o(a)$ elements.

6) Show that any group with atmost 5 elements is abelian

Soln: Groups with order 2, 3, 5 (prime) are abelian.

A group with order 1 i.e.. $G = \{e\}$ is also abelian.

Consider a group of order 4. i.e., $O(G) = 4$

Let $a \neq e \in G$

Let $H = (a)$

Then $O(H) = 1$ or 2 or 4 ($\because O(H) | O(G)$)

ie $a \neq e \rightarrow O(H) = 2$ or 4

Suppose $O(H) = 4 = O(G) \Rightarrow G = H = (G)$

$\Rightarrow G$ is cyclic $\Rightarrow$ abelian

If $O(H) = 2$, H has only 2 elements say $e \& a$. Both e and a are its own inverse

$\Longrightarrow H$ is abelian

$G = \{ a \; e \; b \; c \}$ where $a^{-1} = a$, $e^{-1} = e$ & $b^{-1} = c$

Show that G is abelian.

$b * c = b * b^{-1} = e$

$c * b = b^{-1} * b = e \longrightarrow b * c = c * b$

Now, $a * b = C$ (As $a * b \neq e, a, b$)

Similarly $b * a \neq a, b, e$

$b * a = C$

$a * b = b * a$

Also we get $a * C = C * a$

$\longrightarrow G$ is Abelian