Cyclic Groups

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

Examples:

① In $(Z, +)$, $\langle 2 \rangle = 2Z$ which is the group of even integers

$2Z = \{\ldots -4, -2, 0, 2, 4, 6, \ldots\}$

$2^1 = 2$; $2^2 = 4$; $2^3 = 8$ . . . . .

Hence $a^n = 2^n = 2Z = H$, $n \in Z$. is a Subgroup of G.

② In the group $G = (Z_{12}, \oplus)$ $\langle 3 \rangle = \{0, 3, 6, 9\}$

$\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$

③ In the group $G = \{1, i, -1, -i\}$

$\langle i \rangle = \{i, i^2, i^3 \ldots\} = \{i, -1, -i, 1\} = G.$

Theorem 3.22.

Any Cyclic group is abelian.

Let $G = \langle a \rangle$ be a Cyclic group

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

Hence $xy = a^m \cdot a^n = a^{m+n}$

$= a^{n+m}$

Scanned with CamScanner

∴ Hence G is abelian.

Theorem 3.23

A subgroup of cyclic group is cyclic.

Let G be a cyclic group $\langle a \rangle$ generated by a and let H be a subgroup of G.

To prove that H is cyclic

Clearly every element of H is of the a^n for some integer $n \in \mathbb{Z}$.

Let m be the smallest positive integer such that $a^m \in H$. $\langle a^m \rangle$

To prove that a^m is a generator of H.

Let $b \in H$. Then $b = a^n$ for $n \in \mathbb{Z}$.

Let $n = mq + r$ where $0 \leq r < m$.

Then
$$b = a^n$$
$$= a^{mq+r}$$
$$= a^{mq} \cdot a^r$$
$$= (a^m)^q \cdot a^r$$

$$b(a^m)^{-q} = a^r \longrightarrow (1)$$

Now $a^m \in H$. since H is subgroup. then $(a^m)^{-q} \in H$, and also $b \in H$

by (1) $a^r \in H$. and $0 \leq r < m$.

~~m~~ is the smallest positive integer such that $a^m \in H$

$\therefore r=0$ Hence $b = a^n = a^{mq+r}$

$= a^{mq} \cdot a^r$

$= a^{mq} \cdot a^0$

$= a^{mq}$

$b \quad = (a^m)^q$

$b \in H$

$\therefore$ every element of H is a power of (a^m)

$H = \langle a^m \rangle$ and Hence H is cyclic

3.7. Order of an element

Definition :

Let G be a group and let $a \in G$. The least positive integer n (if it exists) Such that $a^n = e$ is called order of a. If there is no positive integer n such that $a^n = e$, then the order of a is said to be infinite.

~~Theo~~ Example : 1. $(C^*, \cdot)$ i is an element of order 4.

$G = \{1, -1, i, -i\}$

$i^4 = 1$ least

$i^8 = 1$

$i^{12} = 1$.

$\therefore o(i) = 4$

$\boxed{\text{Theorem 3.24}}$

Let G be a group and $a \in G$. The order of a is same as the order of the cyclic group generated by a

Let a be an element of order n

Then $a^n = e$. n is least positive integer

To prove that $e, a, a^2, \ldots a^{n-1}$ are all distinct

Suppose $a^r = a^s$ where $0 < r < s < n$.

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

$$e = a^{s-r} \quad \text{and} \quad s-r < n.$$

Since n is least positive integer. which is contradicts the definition of the order of a. $\therefore a^r \neq a^s$.

Hence $e, a, a^2, \ldots a^{n-1}$ are n distinct elements and $\langle a \rangle = \{ e, a, a^2, \ldots a^{n-1} \}$ which is of order n.

$$\therefore o(G) = o(a) = n.$$

If a is of infinite order the sequence of elements $a, a^2, \ldots a^n, \ldots$ are all distinct and are in $\langle a \rangle$.

Hence $\langle a \rangle$ is an infinite group.

Theorem 3.25.

In a finite group every element is of finite order.

Let $a \in G$. If a is of infinite Order, then $\langle a \rangle$ is an infinite subgroup of G, which is a Contradiction G is finite, Hence the order of a is finite.

Scanned with CamScanner

Theorem 3.26

Let G be a group and a be an element of order n in G. Then $a^m = e$ iff n divides m.

we know that $o(a) = n \Rightarrow a^n = e$

If n/m (n divides m). Then $m = nq$ where $q \in \mathbb{Z}$ [q is positive integer].

$$a^m = a^{nq} = (a^n)^q = e^q = e$$

$\therefore a^m = e$.

Conversely, let $a^m = e$

Let $m = nq + r$ where $0 \leq r < n$

$$a^m = a^{nq+r} = a^{nq} \cdot a^r = e \cdot a^r = a^r$$

$\therefore a^r = e$ and $0 \leq r < n$

n is least positive integer such that $a^n = e$ we have $r = 0$. Hence $m = nq$

$\therefore$ Therefore n/m.

Theorem 3.27.

Let G be a group and $a, b \in G$

Then (i) Order of a = order of a^{-1}

(ii) Order of a = Order of $b^{-1}ab$

(iii) Order of ab = order of ba

(i) Let a be an element of order n.

Then $a^n = e$

To prove $(a^{-1})^n = e$ and n is least positive integer.

let $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$.

$\therefore (a^{-1})^n = e$.

Now, if possible let $0 < m < n$ and

Scanned with CamScanner

$(a^{-1})^m = e$

$(a^m)^{-1} = e$ Hence $a^m = e$ which Contradicts the definition of order of a

$\therefore a^n = e$. Thus n is the least positive integer such that $(a^{-1})^n = e$

$\therefore$ The order of a^{-1} is n.

(ii)

We shall first prove that for any positive integer r then $(b^{-1}ab)^r = b^{-1}a^r b$. $\to$ ①

Let $r=1$ then $(b^{-1}ab)^1 = b^{-1}a^1 b$.

$b^{-1}ab = b^{-1}ab$.

$r=1$) is trivial true.

Now ① is true for $r=k$ so that

$(b^{-1}ab)^k = b^{-1}a^k b$. put $r = k+1$.

Then $(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$

$= b^{-1}a^k b b^{-1} a b$.

$= b^{-1}a^k a^1 b$.

$= b^{-1}a^{k+1} b$.

Hence by induction ① is true for all positive integers.

Let a be any element of order n. Then $a^n = e$.

$(b^{-1}ab)^n = b^{-1}a^n b = b^{-1}eb = e$.

Now, if possible let $0<m<n$ and $(b^{-1}ab)^m = e$.

$\therefore (b^{-1}ab)^m \Rightarrow b^{-1}a^m b = e$

$\Rightarrow bb^{-1}a^m b = be$ (Pre multiple by b on both sides)

$e a^m b = b$

$a^m b b^{-1} = b b^{-1}$ (post multiply by b^{-1} on both sides)

$a^m = e$

which contradicts the definition of the order a. Thus n is least positive integer such that

$$(b^{-1} ab)^n = e.$$

$\therefore$ The order of $b^{-1}ab$ is n.

(iii) put $b = a$ and $a = ab$. then.

$$(a^{-1} ab a) = (a^{-1} a) ba = eba = ba.$$

$\therefore$ The order of ab = the order of ba.

$\boxed{\text{Theorem } 3\cdot 28}$.

let G be a group and let a be an element of order n in G. Then the order of a^s, where $0 < s < n$ is n/d, where d is the greatest common divisor of n and s.

Let $n/d = k$ and $s/d = l$

so that k and l are relatively prime.

Now, $(a^s)^k = a^{sk} = a^{ldk} = a^{ln} = (a^n)^l = e$

Further if m is any positive integer such that

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

$$a^{sm} = e$$

since order of a is n, we have n/sm.

$a^n = e$

$a^{sm} = e \Rightarrow n / sm$

$\therefore$ $kd / ldm \Rightarrow k / lm$

But k and l are relatively prime.

Hence k / m so that $m \geq k$

Thus k is the least positive integer such that $(a^s)^k = e$

$\therefore$ order of $a^s = k = n/d$.

Cosets and Lagrange's Theorem

Definition

Let H be a subgroup of a group 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 the right coset of H defined by a.

Examples :

2. Consider $(Z_{12}, \oplus)$. Then $H = \{0, 4, 8\}$ subgroup of G.

The left cosets of H are given by

$0 + H = \{0, 4, 8\} = H$.

$1 + H = \{1, 5, 9\}$

$2 + H = \{2, 6, 10\}$

$3 + H = \{3, 7, 11\}$

$4 + H = \{4, 8, 0\} = H$

$5 + H = \{5, 9, 1\} = 1 + H$.

Scanned with CamScanner

Theorem. 3.29

Let G be a group and H be a subgroup of G. Then.

(i) $a \in H \Rightarrow aH = H$

(ii) $aH = bH \Rightarrow a^{-1}b \in H$

(iii) $a \in bH \Rightarrow a^{-1} \in Hb^{-1}$

(iv) $a \in bH \Rightarrow aH = bH$.

Proof:

(i) Let $a \in H$. To prove that $aH = H$.

let $x \in aH$ Then

$x = ah$ for all $h \in H$

Now, $a \in H$ and $h \in H$. $\Rightarrow ah = x \in H$.

Since H is subgroup.

Hence $aH \subseteq H$

let $x \in H$ then

$ex \in H$

$a(a^{-1}x) \in H$

$x = a(a^{-1}x) = aH$. Hence $H \subseteq aH$.

Thus $H = aH$.

Conversely, let $aH = H$. Now,

$a = ae \in aH$. for all $e \in H$.

$\therefore a \in H$.

(ii) let $aH = bH$.

pre multiply by a^{-1}.

$a^{-1}aH = a^{-1}(bH)$

$H = (a^{-1}b)H$.

Since H is subgroup. then

$a^{-1}b \in H$ by (i)

Conversely let $a^{-1}b \in H$.

Then $a^{-1}bH = H$ (by i)

(pre multiply by a)

$$(aa^{-1})bH = aH$$

$$bH = aH.$$

(iv) let $a \in bH$. To prove that $aH = bH$.

let $x \in aH$

$x = ah_1$ for some $h_1 \in H$. $\rightarrow$ (1)

Also $a \in bH$. $\Rightarrow a = bh_2$ for some $h_2 \in H$.

Then $x = (bh_2)h_1$ from (1).

$x = b(h_2h_1)$

$x = bh_3$ for some $h_3 \in H$

$x \in bH$.

$\therefore aH \subseteq bH$.

Now, let $x \in bH$ Then

$x = bh_1$ for some $h_1 \in H$.

Then also $b \in aH \Rightarrow b = ah_2$ for some $h_2 \in H$

$x = (ah_2)h_1$

$x = a(h_2h_1)$

$x = ah_3$ $\therefore h_3 \in H$

$x \in aH$

$\therefore bH \subseteq aH$. Hence $aH = bH$.

Conversely, let $aH = bH$.

Then $a = ae \in aH$.

$a \in bH$.

Scanned with CamScanner

(iii) Let $ab \, a \in bH$. Then

$\Leftrightarrow \quad a = bh$ for some $h \in H$.

$\Leftrightarrow \quad a^{-1} = (bh)^{-1}$

$\Leftrightarrow \quad a^{-1} = h^{-1}b^{-1}$

Since H is subgroup of G.

$\Leftrightarrow \quad a^{-1} \in Hb^{-1}$

Theorem 2.30:

Let H be a subgroup of G. Then

(i) any two left cosets of H are either identical or disjoint

(ii) Union of all the left cosets of H is G

(iii) the number of elements in any left coset aH is the same as the number of elements in H.

Proof:

(i) Let aH and bH be two left cosets.

Suppose aH and bH are not disjoint

we claim that $aH = bH$.

Since aH and bH are not disjoint

$$aH \cap bH \neq \phi$$

There exists an element

$$c \in aH \cap bH.$$

$c \in aH$ and $c \in bH$.

$ce \in aH$ and $ce \in bH$ since H is SG.

$cH = aH$ $\qquad$ $cH = bH$.

Hence $aH = bH$.

Scanned with CamScanner

(ii) Let $a \in G$. Then
$a \in aH$.
every element of G belongs to a left coset of H.
Hence the union of all the left cosets of H is G.

(iii) The map $f : H \to aH$ defined by
$f(h) = ah$. is clearly bijection

(a) To prove f is 1-1.
$f(h_1) = f(h_2)$
$ah_1 = ah_2$
$h_1 = h_2$ (by left cancellation law)

(b) To prove f is onto.
Choose $ah \in aH$.
$h \in H$.
By definition of 'f' is. $f(h) = ah$.
h is preimage of ah.
$\therefore f$ is onto

Hence every left coset has the same number of elements as H.

Remark

Let H be a subgroup of G. we define a relation in G as follows.
Define $a \sim b \Leftrightarrow a^{-1}b \in H$.
Then $\sim$ is a equivalence relation.
For $a^{-1}a = e \in H$. Hence $a \sim a$;
Hence $\sim$ is reflexive.

Scanned with CamScanner

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

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

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

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

$\Rightarrow b \sim a$

Hence $a \sim b \Rightarrow b \sim a$.

Hence $\sim$ is symmetric.

Now

$a \sim b$ and $b \sim c$

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

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

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

$\Rightarrow a^{-1}ec \in H$

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

$\Rightarrow a \sim c$

Hence $\sim$ is transitive.

Thus $\sim$ is an equivalence relation.

Now we claim that equivalence class $[a] = aH$.

Let $b \in [a]$ Then $b \sim a \Rightarrow a \sim b$

$a^{-1}b \in H$

$a^{-1}b = h$ for some $h \in H$

$a a^{-1}b = ah$

$e\, b = ah.$ (pre multiply by a on both sides)

$b = ah$

Hence $b \in aH$

Scanned with CamScanner

Also, $b \in aH$

$\Rightarrow \quad b = ah$ for some $h \in H$.

$\Rightarrow \quad a^{-1}b = a^{-1}ah$ (pre multiply by a^{-1} on both sides)

$\Rightarrow \quad a^{-1}b = h$

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

$\Rightarrow \quad a \sim b$

$\Rightarrow \quad b \in [a]$. Hence $[a] = aH$

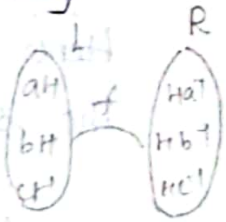
Theorem 3.31

Let H be a subgroup of G. The number of left cosets of H is the same as the number of right cosets of H.

Let L and R respectively denote the set of left and right cosets of H.

we define map $f : L \to R$ by

$f(aH) = Ha^{-1}$



f is well defined

for $aH = bH \Rightarrow a^{-1}b \in H$ by theorem 3.29. $aH = bH \Rightarrow a^{-1}b \in H$

$\Rightarrow a^{-1} \in Hb^{-1}$

$Ha^{-1} = Hb^{-1}$

$f(aH) = f(bH)$.

f is 1-1 for.

$f(aH) = f(bH)$

$\Rightarrow Ha^{-1} = Hb^{-1}$

$\Rightarrow \quad a^{-1} \in Hb^{-1}$ (by theorem 3.29)

Scanned with CamScanner

$\Rightarrow a^{-1} = hb^{-1}$ for some $h \in H$

$\Rightarrow (a^{-1})^{-1} = (hb^{-1})^{-1}$

$\Rightarrow a = b h^{-1}$

$\Rightarrow a \in bH$

$\Rightarrow aH = bH$ (by theorem 3.24) (see)

f is onto for every right coset Ha has a preimage under f namely $a^{-1}H$.

Let $Ha^{-1} \in R$

$H \in H$, $a^{-1} \in G$

$(a^{-1})^{-1} \in G$

$a \in G$

$aH \in L$

$\therefore f(aH) = Ha^{-1}$

Hence f is a bijection from L to R.
Hence the number of left cosets is the same as the number of right cosets.

<u>Definition</u>

Let H be a subgroup of G. Then The number of distinct left or right Cosets of H in G is called Index of H in G and is denoted by $[G:H]$.

Example:

In $(Z_8, \oplus)$, $H = \{0, 4\}$ is a Subgroup of the left cosets of H are given by,

Scanned with CamScanner

$$\begin{cases} 0+H = \{0,4\} \\ 1+H = \{1,5\} \\ 2+H = \{2,6\} \\ 3+H = \{3,7\} \end{cases}$$

$4+H = \{4,0\} = H$

$5+H = \{5,1\} = 1+H.$

These are the four distinct left cosets of H.

Hence the index of subgroup H is 4.

$$\frac{O(G)}{O(H)} = \frac{8}{2} = 4$$

Theorem 3.32

Lagrang's theorem.

Let G be a finite group of order n and H be any subgraup of G. Then the order of H divides the order of G.

Let $|H| = m$ that is $o(H) = m$ and $o(G) = n$. and $[G:H] = r$.

Then the number of distinct left cosets of H in G is r.

By our known theorem "The number of elements in any left coset aH is the same as the number of elements in H.".

Also these r left cosets are mutually disjoint, they have same number of elements namely m and their union is G

$n = rm$

Hence m divides n.

Theorem 3.22

The order of any element of a finite group G divides the order of G.

Let G be a group of order n. $O(G) = n$.

Let $a \in G$ be an element of order m. $O(a) = m$.

Then the order of a is same as the order of the cyclic group $\langle a \rangle$

that is $O(a) = \langle a \rangle$.

by our Known theorem ~~the number~~

" Let G be a finite group of order n and H be any subgroup of G. Then the order of H divides order of G "

The order of subgroup $\langle a \rangle$ divides $O(G)$

m divides n.

Theorem: 3.34. Every group of prime ~~The~~ order of any is cyclic.

Let G be a group of order p. $O(G) = p$. where p is prime

Let $a \in G$ and $a \neq e$

By our known theorem the order of any element of a finite group G divides the order of G.

$\frac{O(G)}{O(a)}$ $O(a) / O(G)$. order of a divides p.

$\frac{p}{O(a)}$ $\Leftarrow O(a) / p$. order of a is 1 or p.

since $a \neq e$ order of a is p.

Hence $G = \langle a \rangle$ so that G is cyclic.

Theorem 3.35

Let G be a group of order n. let $a \in G$. then $a^n = e$.

Let the order of a be m. Then m divides n. Hence $n = mq$.

$$a^n = a^{mq} = (a^m)^q = e^q = e.$$

$$\therefore \boxed{a^n = e}$$

Theorem 3-36.

__Euler's theorem.__

If n is any integer and $(a,n) = 1$ then $a^{\phi(n)} = 1 \pmod{n}$.

Let $G = \{ m / m < n \text{ and } (m,n) = 1 \}$.

G is a group under multiplication modulo n.

This group is of order $\phi(n)$.

Now let $(a,n) = 1$.

let $a = qn + r$; $0 \leq r < n$. So that

$O(G) = n$

$a^n = e$

$a = r \pmod{n}$.

$O(G) = \phi n$

since $(a,n) = 1$ we have

$r^{\phi n} = 1$

$(n, r) = 1$. so that $r \in G$.

$r^{\phi(n)} = 1$ (by our known theorem)

$$r^{\phi(n)} \equiv 1 \pmod n$$

also

$$a^{\phi(n)} \equiv r^{\phi(n)} \pmod n$$

So that

$$a^{\phi(n)} \equiv 1 \pmod n$$

since "$\equiv$" is transitive.

Theorem 3.38.

A group G has no proper subgroups iff it is a cyclic group of prime order.

Proof

Suppose G is a cyclic group of prime ord.

To prove G has no proper subgroups.

let $O(G) = p$

Then by Lagrange's theorem $O(H) \mid O(G)$

Since $O(G) = p$ where p is prime.

$O(H) = 1$ or p.

$H = \{e\}$ (or) $H = G$

H is a improper subgroup.

Hence G has no proper subgroup.

Converse part.

Given G has no proper subgroup.

To prove G is a cyclic group of prime order.

Suppose G is not cyclic. let $a \in G$ $a \neq e$.

Then the cyclic group $\langle a \rangle$ is a proper subgroup of G. which is contradiction.

Hence G is cyclic.

Scanned with CamScanner

Also G cannot be infinite, for an infinite cyclic group contains a proper subgroup $\langle a^2 \rangle$. Hence G must be of finite order, say n.

To prove n is prime.

If possible let n be an composite number. let $n = pq$. where $p, q > 1$.

let $a \in G$ be a generator of the group. Then $\langle a^p \rangle$ is a subgroup of order q, and hence proper subgroup of G which is a contradiction.

Hence n is prime.

$\therefore G$ is a cyclic group of prime order.

Theorem 3.37

<u>Fermat's theorem</u>

Let p be a prime number and a be any integer relatively prime to p. Then $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Since p is prime, and let a be any integer relatively prime to p.

$\phi(p) = p - 1$.

Then by Euler's theorem.

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\ n)$$

$$a^{\phi(p)} \equiv 1 (\mathrm{mod}\ p)$$

we know that $\phi(p) = p - 1$

Hence, $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$