Cosets

Let G be a group and H be a subgp of G. For any $a \in G$

$Ha = \{ha \mid h \in H, a \in G\}$ ⟶ Right coset of H in G

$aH = \{ah \mid a \in G, h \in H\}$ ⟶ Left coset of H in G

of the binary operation is $*$, Then the cosets are

$Ha = \{h * a \mid h \in H, a \in G\}$ and $aH = \{a * h \mid h \in H, a \in G\}$

Theorem 1 :

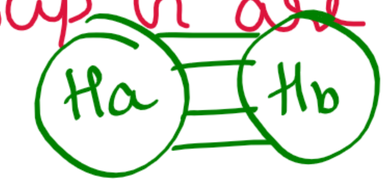
Let G be a geoup and H be a subgeoup. Then any 2 right cosets are either identical or disjoint

Equivalently,

Any 2 left cosets are either identical or disjoint.

Theorem 2:

Any two right cosets of a subgroup H in a group G are in one-to-one correspondance with each other



Proof :-

Let H be a subgroup of G and let $a, b \in G$ s.t $a \neq b$ consider a distinct right cosets Ha and Hb in G.

we've to s.T, there exists a function $f : Ha \to Hb$ which is one one & onto

Define $f : Ha \longrightarrow Hb$ by $f(ha) = hb \ \forall \ h \in H$

f is one one :- If $f(x) = f(y) \Rightarrow x = y$

If $f(x) = f(y)$ where $x, y \in Ha$

$x = h_1 a$ & $y = h_2 a$

$$f(h_1 a) = f(h_2 a)$$

$$h_1 b = h_2 b$$

$$h_1 = h_2$$

$$h_1 a = h_2 a$$

$$x = y$$

f is onto :-

Let $hb \in Hb \Rightarrow h \in H$

$\Rightarrow ha \in Ha$

$\therefore$ If every image $hb \in Hb$, $\exists$ a preimage $ha \in Ha$ s.t $f(ha) = hb$.

$f : Ha \longrightarrow Hb$ is one one & onto

$\therefore$ Bijection

Theorem 3:

Let H be a subgroup of G. Then any 2 right cosets of H in G have same (finite or infinite) no of elts

Proof:-

Proof of theorem 2.

Theorem 4:

Any two left cosets of a subgp H in G are in one to one correspondance with each other

OR

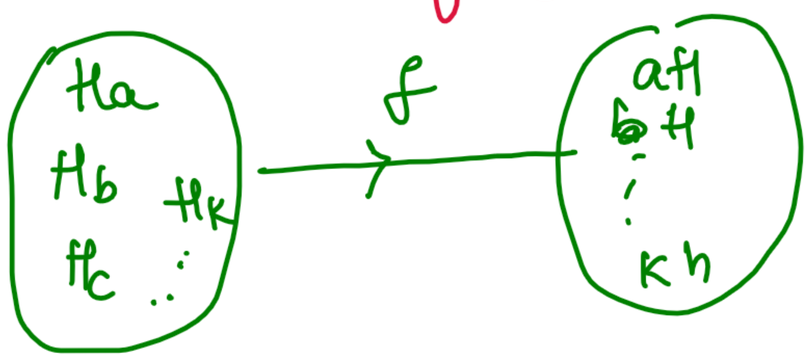
Any two left cosets of a subgroup H in G have same no of elts.

Proof:-

similar to that of Theorem 2.

Theorem 5:

Suppose H is a subgp of G. Then the no of distinct left cosets of H in G is equal to the no of distinct right cosets of H in G



OR

There exists one to one corresp b/w the set of all left cosets of H in G and the set of right cosets of H in G

Proof:-

Let $L = \{aH \mid a \in G\}$, set of all left cosets of H in G

$R = \{Ha \mid a \in G\}$, set of all right cosets of H in G

Define a map $f: L \to R$ s.t $f(aH) = Ha^{-1}$ $\forall$ $a \in G$

$f : L \longrightarrow R$

i) f is well defined:

(S.T if $aH = bH$, then $f(aH) = f(bH)$)

If $aH = bH$

$b^{-1}aH = H$

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

$\Rightarrow Ha^{-1}b = H$

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

$\Rightarrow f(aH) = f(bH)$

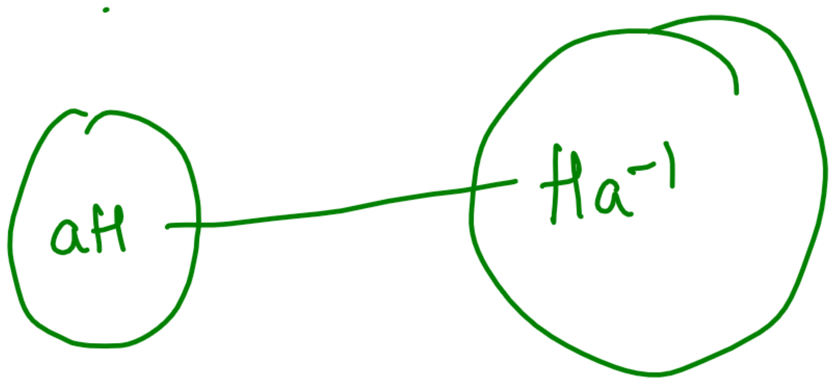
ii) f is one one

(If $f(aH) = f(bH) \Rightarrow aH = bH$)

$f(aH) = f(bH)$

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

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



$H = Hb^{-1}a$ $\quad (aa^{-1} = a^{-1}a = e)$

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

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

Thus $a^{-1}bH = H$ (closure law $a^{-1}b \in H$, $H \subseteq H$
$a^{-1}bH \in H$

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

$bH = aH$

iii) f is onto

(Fd any $Ha \in R$, $\exists\ aH \in L$ s.t $f(\ ) = Ha$)

Fd any $Ha \in R$, $\exists\ a^{-1}H \in L$ s.t

$f(a^{-1}H) = H(a^{-1})^{-1} = Ha$

$\therefore$ f is onto

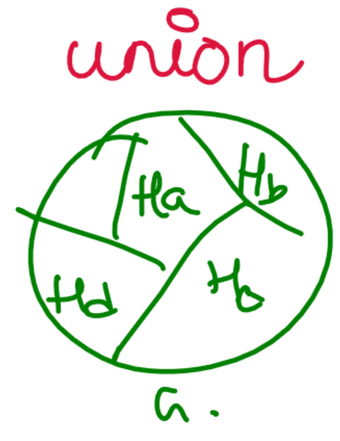
$f : L \longrightarrow R$ s.t f is one one & onto

$\therefore$ $\exists$ one-to-one corresp blw L & R

i.e, L & R same no of elts

Theorem 6

If H is any subgp of G, then G is equal to the union of all right cosets of H in G



Proof:-

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

$$\bigcup_{a \in G} Ha \subseteq G \quad \text{---------} \quad (1)$$

Conversely, if any $a \in G$, $a = ea \in Ha$

i.e $a \in Ha$

$a \in Ha \cup Hb \cup \ldots\ldots$

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

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

From (1) & (2)

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

To prove $A = B$

we must show

$A \subseteq B$

$B \subseteq A$

Lagrange's theorem

Let G be a finite group and H be a subgp of G. Then

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

($o(G) = 5$, Any subgp H will be of ordn 1 & 5

if $o(G) = 4$, then H have ordn 1/2/4)

Proof:-

Since G is finite, the no of left cosets in G is finite

Let $a_1H, a_2H, \ldots a_kH$ be distinct left cosets of H in G

From theorem (5), $G = \bigcup_{a \in G} aH$

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

And any 2 left cosets are disjoint

$$\therefore o(G) = o(a_1H) + o(a_2H) + \cdots + o(a_kH)$$

And any 2 left cosets have same cardinality

and it is equal to the no of elts in H

$o(a_1H) = o(a_2H) = \cdots = o(a_kH) = o(H)$

$$\therefore o(G) = \underbrace{o(H) + o(H) + \cdots + o(H)}_{k \text{ times}}$$

$$= k\,o(H)$$

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

Index of a subgp:-

The no of distinct right cosets of H in G is called the index of H, it is denoted by $i_G(H)$ & $(G:H)$

By Lagranges thm, $i_G(H) = \frac{o(G)}{o(H)} = K$

"A group of prime order has no non trivial subgps"

$o(G) = p \longrightarrow o(H) \Rightarrow 1$ & p

1 ⇓ only $H = G$

* Let $(G, \cdot)$ be a group where $G = \{1, -1, i, -i\}$.
of $H = \{1, -1\}$. Evaluate $i_G(H) = ?$

sol:-

$H_1 = \{1, -1\}$

$H_{-1} = \{-1, 1\}$

$H_i = \{i, -i\}$

$H_{-i} = \{-i, i\}$

} These are 4 distinct right cosets

$\therefore i_G(H) = 2$

OR

$$i_G(H) = \frac{o(G)}{o(H)} = \frac{4}{2} = 2$$

② $G = \{1, \omega, \omega^2\}$, $(G, \cdot)$ is a group

$\omega \rightarrow$ cube root of unity

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$o(G) = 3$

$\{(1, \omega, \omega^2), \cdot\}$

$1^{-1} = 1$ $\quad \omega^{-1} = \omega^2$

$(\omega^2)^{-1} = \omega$

$(G,\cdot)$ has no nontrivial subgp

Problem

Let G be a group and $a \in G$. Let $H = \{a^n / n \in Z\}$

P.T H is a subgp of G

Proof:-

$a^0 = e \in H$

Thus H is nonempty

To prove that H is a subgp. P.T $\longrightarrow$ $xy^{-1} \in H$ $\forall$ $x, y \in H$

Let $x, y \in H$ ie $x = a^m$ and $y = a^n$ for some $m, n \in Z$

Consider $xy^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n}$

since $m-n \in Z$, $a^{m-n} \in H$

$\therefore$ H is a subgp of G

Cyclic group

A group G is said to be cyclic if there exits an elt $a \in G$ s.t every elt of G can be written as power of 'a'. Then the elt a is called the generator of G. and is written as $G = (a)$

ex:- $G = \{1, -1, i, -i\}$ is cyclic generated by i

ie $G = (i)$

a

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

Theorem

A cyclic group is abelian

Proof:-

Let G be a cyclic group. Then $\exists\ a \in G$ such that $G = (a)$

Let $x, y \in G \Rightarrow x = a^m,\ y = a^n$ fδ $m, n \in Z$

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

$\therefore$ commutative law is true

$\therefore$ Abelian.

Theorem : Every group of prime order is abelian

proof :-

It is enough if we prove that (every gp of prime order is cyclic)

as every cyclic gp is abelian

Let G be a group s.t $o(G) = p$, a prime no

Then $\exists$ an elt $a \in G$ s.t $a \neq e$

Let $H = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$ ⟶ H is a subgp of G

Then H is a subgp of G

By Lagrange's thm, $o(H) = 1$ or p

since $a \neq e$, $o(H) \neq 1$ $\therefore o(H) = p = o(G)$

$\therefore G = H$ ie $G = \langle a \rangle$

$\therefore$ G is cyclic

$\therefore$ G is abelian

converse is not true,

Every cyclic gp is not of prime order

ex:- $(\{1, -1, i, -i\}, \cdot)$ has order 4 & is cyclic

Prob: Any group with atmost 5 elts is abelian

1 trivial ✓ 2 prime ✓ 3 prime ✓ 4 ✗ 5 prime ✓

soln

w.k.t every gp of prime order is abelian

i.e Gps of order 2, 3, 5 are abelian

If $o(G) = 1 \Rightarrow G = \{e\}$, this is abelian ✓

If $o(G) = 4 \Rightarrow$

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

Let $H = (a)$. Then $o(H) = 1$ or 2 or 4

- since $a \neq e$, $o(H) \neq 1$
- If $o(H) = 4$, $G = H \Rightarrow G = (a)$
  $\Rightarrow G$ is cyclic and hence abelian
  $\Rightarrow G$ is abelian
- If $o(H) = 2$, $H = \{e, a\}$ where $a^{-1} = a$

If $G = \{a, e, b, c\}$ and if every elt is its own inverse $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$

$e^{-1} = e$

Then G is abelian

If $G = \{a, e, b, c\}$ and $a^{-1} = a$, $e^{-1} = e$

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

Then $a * b = b * a = c$ (as it cant be e)

$b * c = c * b = e$ (as they are inv of each other)

Prob

S.T subgp of any cyclic group is again cyclic

Proof:-

Let G be cyclic ie $G = (a)$

Let H be subgp of G, $\Rightarrow$ elts of H are in the form a^n, $n \in \mathbb{Z}$

Let n_0 be the smallest integer s.t $a^{n_0} \in H$

we shall S.T $H = \langle a^{n_0} \rangle$, P.T H is cyclic

Let $x \in H$, then $x = a^m$ for some $m \in \mathbb{Z}$

By dvsn alg, $m = q n_0 + r$, $0 \le r < n_0$

of $r \neq 0$, $r = m - q n_0$ and $a^r = a^{m - q n_0}$

$= a^m \cdot (a^{n_0})^{-q} \in H$

$n_0 \to$ smallest $a^{n_0} \in H$

a contradictn

$\therefore r = 0$ $\therefore$ $m = q n_0 + 0$

$x = (a^{n_0})^q$ for $q \in \mathbb{Z}$

$\therefore x = a^m = a^{q n_0} = (a^{n_0})^q$ $q \in \mathbb{Z}$

$H = (a^{n_0})$

$\therefore$ H is cyclic

order of an elt :-

Let G be a gp and $a \in G$. Then the smallest integer n s.t $a^n = e$ is called order of 'a' & is denoted by $o(a)$

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

$i^4 = 1 \Rightarrow o(i) = 4$

$(-i)^4 = 1 \Rightarrow o(-i) = 4$

$(-1)^2 = 1 \Rightarrow o(-1) = 2$.

Theorem

order of an elt divides order of the gp

proof:-

Let G be a finite gp & $a \in G$

Let $o(a) = n$

consider $H = (a)$

$= \{a, a^2, a^3, \ldots a^{n-1}, a^n = e\}$

clearly $o(H) = n = o(a)$

Hence H has atmost n elts

If $a^i = a^j$ for $0 \le j < i < n$

$a^{i-j} = e$ $\quad 0 \le i - j < n$, a contradictn to the fact $o(a) = n$

$\therefore a^j \neq a^i$

$\therefore o(H) = n$

$\therefore o(H) \mid o(G)$ (Lag thm)

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

---

* Let G be a gp & $a \in G$

$$a^{o(G)} = e$$

Proof:-

Let $o(a) = n$, ie.

$o(G) = q\,o(a) = nq$ $\left(\because o(a) \mid o(G)\right.$

consider $a^{o(G)} = a^{nq} = (a^n)^q = e^q$

$= \underline{e}$

* S.T $Z_5 = \{0, 1, 2, 3, 4\}$ forms a cyclic gp under the operatn of addn modulo 5 ($\oplus_5$)

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

Identity elt : 0

Inverse :

$0^{-1} = 0$

$1^{-1} = 4$

$4^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

Lets find the generatd.

(1) $\Rightarrow 1^0 = 0$

$1^1 = 1$

$1^2 = 1+1 = 2$

$1^3 = 1+1+1 = 3$

$1^4 = 1+1+1+1 = 4$

$\therefore$ gen 1 gives all elts

(2) $= 2^0 = 0$

$2^1 = 2$

$2^2 = 4$

$2^3 = 1$

$2^4 = 3$

$\therefore$ 2 is a generatd

We can verify that all the elts expt 0 are generatds

2nd

Note:

$(Z_n, \oplus_n)$ is cyclic and all the elts which are relatively prime to n are generatds.