U19CS076

Tutorial 1
Group Theory

EXAMPLES FROM HERSTEIN

1. a) G = set of all integers, $a \cdot b = a - b$

→ If $a, b \in G \Rightarrow a, b \in Z$
$a \cdot b = a - b \in Z$
$\Rightarrow a \cdot b \in G$

Closed

→ If $a, b, c \in G$
$a \cdot (b \cdot c) \Rightarrow a - (b - c) = a - b + c$
$(a \cdot b) \cdot c \Rightarrow (a - b) - c = a - b - c$
$\neq (a \cdot b) \cdot c$

NOT Associative

→ If $a \cdot e = a$ for $\forall a \in G$
$\Rightarrow a - e = a$
if $e = 0$
$a \cdot e = a \rightarrow e \in G$

Identity exists

→ If $a \cdot a^{-1} = e$
$a - a^{-1} = 0$
$a^{-1} = a$
$\forall a \in G, a^{-1} \in G$

Inverse exist

→ NOT a group

b) G is set of +ve integers
$a \cdot b = ab$

→ If $a, b \in G \rightarrow a, b \in Z^+$
$a \cdot b = ab \rightarrow ab \in Z^+$
$\Rightarrow ab \in G$

Closure

→ If $a, b, c \in G$

$a \cdot (b \cdot c) = a \cdot (bc) = abc$

$(a \cdot b) \cdot c = (ab) \cdot c = abc$

Associative

→ If $a \cdot e = a = e \cdot a$

$ae = a$

$\Rightarrow e = 1 \quad e \in G$

$\forall a \in G, e \in G$

Identity exist

→ If $a \cdot a^{-1} = a^{-1} \cdot a = e$

$aa^{-1} = 1$

$a^{-1} = 1/a$

Inverse is a rational numbers

$a^{-1} \notin G$

Not a group

c) $G = a_0, a_1 \dots a_6$ where

$a_i \cdot a_j = a_{i+j} \quad i+j < 7$

$a_i \cdot a_j = a_{i+j-7} \quad i+j \geq 7$

→ For ~~any~~ $\cancel{\forall a_n a_m \in G}$ ~~any~~ $\forall a_n, a_m \in G$

$\cancel{a_n \cdot a_m = }$

→ Cyclic Group

Closure group

→ For $a_x, a_y, a_z \in G$

$a_x \cdot (a_y \cdot a_z) = a_x \cdot (a_{y+z})$

$= a_{x+y+z}$

$(a_x \cdot a_y) \cdot a_z = (a_{x+y}) \cdot a_z = a_{x+y+z}$

Associative

$\rightarrow$ For $\forall a_x \in G$

$a_x \cdot a_e = a_e \cdot a_x = a_x$

$a_{x+e} = a_x$

$e = 0$, a_0 is identity element

a_0 is I

$\rightarrow$ For $\forall a_x \in G$

$a_x \cdot a_N = a_e$

$a_{x+N} = a_e$

$N = -x$ $\rightarrow$ not possible

$N = 7 - x$

$a_{x+7-x} = a_7 = a_{7-7} = a_0$

a_{7-x} is inverse.

d) G = set of all rational numbers with odd denom, $a \cdot b = a + b$

$\rightarrow$ For $a, b \in G$

$a \cdot b = a + b$

Denomination will be product of 2 odd

numbers = always odd $\in G$

$\Rightarrow$ Closed

$\rightarrow$ Ass $a \cdot (b \cdot c) = a \cdot (b + c)$

$= a + b + c$

$(a \cdot b) \cdot c = (a + b) \cdot c$

$= a + b + c$

Associative (Denom $= a + b + c =$ odd)

$\rightarrow$ If. $\forall a \in G$

$a \cdot e = e \cdot a = a$

$a + e = e + a = a$

$e = 0 \Rightarrow e = 0/\text{odd number}$

$e \in G$

Identity exists

$\rightarrow$ If $\forall a \in G$

$a \cdot a^{-1} = a^{-1} \cdot a = e$

$a + a^{-1} = a^{-1} + a = e = 0$

$a^{-1} = -a$

$a^{-1} \in G$

Inverse exists

It is a group

(2). If G is abelian group,

$\forall a, b \in G, a \cdot b = b \cdot a$

For $n = 1$, $(a \cdot b)^1 = a^1 \cdot b^1$

Assume $(a \cdot b)^n = a^n \cdot b^n$

then $(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}$

Scanned with CamScanner

$a_1 \; 2$

$a_{14} = a_7 + a_7$

$a_{13} = a$

$$(a.b)^n = a^n . b^n$$

$$(a.b)(a.b)^n = (a.b)(a^n.b^n)$$

$$(a.b)^{n+1} = (a.a^n)(b.b^n)$$

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

$$\Rightarrow (a.b)^n = a^n.b^n \text{ for every } n \geq 0$$

Hence Proved.

Scanned with CamScanner

(3) Given $(a \cdot b)^2 = a^2 \cdot b^2$

$$(ab)(a \cdot b) = a^2 \cdot b^2$$
$$a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$$

[Left & right cancellation]

$$b \cdot a = a \cdot b$$
$$\forall\, a, b \in G \Rightarrow G \text{ is abelian}$$

(9) (a) If Group G is having 3 elements

Order = 3, $a, b \in G$ with $a \neq b$

If $a = e$ (identity)

$$a \cdot b = \cancel{a} \cdot e = e \cdot \cancel{b} = b \cdot a$$

If $b = e$, $b \cdot a = b \cdot e = e \cdot b = a \cdot b$

$$\Rightarrow b \cdot a = a \cdot b$$

Thus when a/b is e it is abelian

When a and b are not identity

$a \cdot b \neq a$ (if $a \cdot b = a \Rightarrow b = e$)

$a \cdot b \neq b$

Since there are only 3 elements say $\{a, b, e\}$

So, due to closure property, they should be inverse each other

$$a \cdot b = e \ \& \ b \cdot a = e$$
$$a \cdot b = b \cdot a$$

$\Rightarrow$ G is abelian for $o(G) = 3$

b) Let $o(G) = 4$ for some $a, b \in G$

If either $a/b = e$

If $a = e \Rightarrow a \cdot b = b = b \cdot a$

$b = e \Rightarrow a \cdot b = a = b \cdot a$

If neither a & b are (e)

$a \cdot b \neq a$, $a \cdot b \neq b$

Let 3rd element be c

$G \rightarrow \{a, b, c, e\}$

so either $a \cdot b = e$ (which means a, b are inverses)

$\Rightarrow a \cdot b = e = b \cdot a$

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

~~a.b =~~ $b \cdot a = b b^{-1} = e$

Or $a \cdot b = c$

Then $a, b \neq e$ and a, b are not inverses

If $a \cdot b = c$

then $b \cdot a$ cannot be a or b or e

so due to closure prop

$b \cdot a = c$

$\Rightarrow$ It is abelian

(c) $o(G) = 5$

Since order of G is prime, G is a cyclic group. Since every cyclic group is abelian

G is abelian

11) If G is a group of even order
Prove it has an element $a \neq e$,
Satisfying $a^2 = e$.

Assume no element is present with
$a^2 = e$ except $a = e$ for $a \in G$
$\Rightarrow a^2 \neq e$ $a \cdot a \neq e$
$\Rightarrow a \neq a^{-1}$

For every non identity element a there exist a^{-1} in a group
So, a can be paired into mutually disjoint subset of order 2.

We assume count of possible subsets = some +ve integer n as G is finite group.

$O(G) = 2n+1$
$\Rightarrow$ Order of G is odd $\rightarrow$ against the Q
$\Rightarrow$ Assumption wrong
There must be an element $a \in G$, $a \neq e$
such that $a^2 = e$ when $O(G)$ is even

(4) Since G is assosiative $\rightarrow$ Semi-group
Let S be finite semigrp.

$S = \{a_1, a_2, a_3 \dots a_n\}$ — ①

Consider any $a_r \in S$ then

$S' = \{a_1 a_l, a_2 a_l \dots a_n a_l\}$
S' belongs to S $\rightarrow$ closure prop.
$O(S') = O(S) = n$
$S' \subseteq S$

If $a_i a_l = a_j a_l$

$a_i \neq a_j$ (All elements of S distinct

for any $a_i \in S$ $\exists$ $a_j \in S \Rightarrow a_i = a_j a_l$

There exists some $a_k \in S$ such that

$a_l = a_k a_l$

$a_i a_l = a_i (a_k a_l) = (a_i a_k) a_l$

Right cancell $a_i = a_i a_k$ a_k is identity right — (1)

We can similarly find $a_* a_i = a_* \; \forall i$ — (2)

a_* is left identity

Thus $a_k = a_* a_k = a_*$.

$a_k = a_*$ Left identity = right identity

If $i = k$ in (1)

$\exists a_m$ such $e = a_k = a_m a_l$

$i = k$ in (2)

$\exists a_n$ such $e = a_n = a_n a_l$

$a_n = a_m = a_l^{-1}$

Since the group has identity & inverse, it is a Group

20. Let G be set of all real 2×2 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $ad - bc \neq 0$ is a rational

Prove G is group under multiplication

→ Closure law,

For $a, b \in G$ ~~a * b~~

$a \cdot b = a * b$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$$

$$D = (ad-bc)(ps-qr) \neq 0$$

Closure

→ For matrix $A, B, C \in G$

$$A\cdot(B\cdot C) = A\cdot(BC) = ABC$$

$$(A\cdot B)\cdot C = AB\cdot C = ABC$$

→ Let identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$|I| \neq 0, \quad I \in G$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Identity exist

→ For inverse $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$

$$A^{-1} = \frac{Adj(A)}{|A|} = \frac{\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}{ad-bc}$$

$A \cdot A^{-1} = e = A^{-1} \cdot A$

$\Rightarrow$ Inverse exists

$\Rightarrow$ $(G, *)$ is ~~at~~ a group.

21. $G = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$

$\rightarrow$ Closure

$(ad - b \times 0 = ad) \in G$

For all $a, b \in G$

$a \cdot b = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} p & q \\ 0 & r \end{bmatrix}$

$= (ad)(pr) \neq 0$

$a \cdot b \in G$

Closure satisfied

$\rightarrow$ Associative

For $a \cdot (b \cdot c) = a \cdot [(ad)(pr)]$

$= (xy)(ad)(pr)$

$(a \cdot b) \cdot c = (xyad) \cdot pr$

$= xyadpr$

$\rightarrow$ Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$a \cdot e = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = ad$

$e \cdot a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = ad$

Identity exist

→ For inverse

$$A^{-1} = \frac{Adj(A)}{|A|} = \frac{\begin{bmatrix} d & -b \\ -a & 0 \end{bmatrix}}{ad}$$

$$|A^{-1}| = \frac{1}{|A|} = \frac{1}{ad} \neq 0$$

$$A^{-1} \in G$$

$$A \cdot A^{-1} = e = A^{-1} A$$

Inverse exists

⇒ G is a group under multiplication

22) $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$

→ Closure

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & a^{-1}b^{-1} \end{bmatrix} \in G$$

→ Associativity holds for all matrices

→ Identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$A I = A$$

→ $A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$ $\quad A^{-1} = \frac{adj(A)}{|A|} = \frac{\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}}{}$

Inverse exists

$\rightarrow$ G is a group.

(24). Let $G = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc \neq 0$

Using matrix multiplication P.T $O(G) = 6$.

a, b, c, d modulo 2 can be 0 or 1

Also $ad - bc \neq 0$

$\cancel{ad} \neq bc$

$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right.$

$O(G) = 6$

(25). a) No. of ways to find $a, b, c, d = 0$

$ad - bc = 0$.

$\rightarrow$ $ad - bc = 0 \rightarrow$ No. of ways of finding $ad = 0 \rightarrow 6 - 1 = 5$

No. of ways of finding $bc = 0$.

$6 - 1 = 5$

Total ways $= 5 * 5 = 25$

$\rightarrow$ $ad - bc \neq 0 \rightarrow$ No. of ways of ~~finds~~ finding a. $= 2$

No. To find $a = 2$

To find $b = 2$

" " " $c = 2$

" " " $d = 1$

Total ways $= 2 \times 2 \times 2 \times 1 = 8$

$O(G) = 34 - 25 - 8 = 48$

b) No. of ways in which $ad - bc = 1$ are

i) $ad = 0 \rightarrow bc = -1$. Ways to find $ad = 5$

Ways to find $bc = 2$

ii) $bc = 0 \Rightarrow ad = -1$

Ways to find $ad = 2$

$bc = 5$

iii) $ad \neq 0 \Rightarrow bc \neq 0$

Ways to find $ad = 2$

" " find $bc = 2$

Total ways $= 20 + 4 = 24$

$\therefore o(G) = 24$

~~$\Rightarrow o(G$~~

(26) a) No. of ways in which $ad - bc = 0$

i) $ad - bc = 0$

No. of ways in which $ad = 0$

$\Rightarrow 2p - 1$

Total ways $= (2p-1)^2$

ii) $ad = bc = 0$

No. of ways of choosing $a = (p-1)$

Total way $= (p-1)^3$

No. of ways of chossing a, b, c, d such $ad - bc \neq 0$

$\Rightarrow p^4 - (2p-1)^2 - (p-1)^3$

$o(G) = p^4 - p^3 - p^2 + p$

b) No. of ways in which $ad - bc = 1$

$\Rightarrow ad = 0, \; bc = -1 \rightarrow$

Total ways $= (2p-1)(p+1$

$bc = 0 \to ad = 1$

$\Rightarrow$ Total ways $= (2p-1)(p-1)$

$ad \neq 0$ & $bc \neq 0$

$\Rightarrow$ No. of ways of choosing $ad = p-1$

No. of ways $bc = p-1$

Total way $= (p-1)(p-1)$

No. of ways $= (2p-1)(p-1) + (2p-1)(p-1) + (p-1)(p-1)$

$$o(G) = p^3 - p$$

---

1. Let $(G, *)$ be a group. Prove
   a. Identity element is unique in $(G, *)$
   b. Inverse of a^{-1} is a, $a \in G$
   c. Left cancellation
   d. Right cancellation

(a). G has to contain atleast one identity element. Suppose both e, e' are identity element in G.

As e is identity

$$e * e' = e \quad — (1)$$

e' is identity

$$e' * e = e \quad — (2)$$

$$\Rightarrow e = e' \quad \text{From } (1), (2).$$

Thus identify element is unique.

(b). If $a \in G$, then $a^{-1} \in G$

$$a * a^{-1} = e$$

Scanned with CamScanner

$\rightarrow a^{-1} * a = e$

So $(a^{-1})^{-1} = a$

(c). Let $a, b, c \in G$ and $a * b = a * c$

$$b = e * b$$
$$= (a * a^{-1}) * b$$
$$= a^{-1} * (a * b)$$
$$= a^{-1} * (a * c)$$
$$= e * c$$

$\therefore b = c$

Left cancellation law

(d). Let $a, b, c \in G$ and $b * a = c * a$

$$b = b * e$$
$$= b * (a * a^{-1})$$
$$= (b * a) * a^{-1}$$
$$= (c * a) * a^{-1} = c * e$$
$$= c$$

$b = c$

$\rightarrow$ Right cancellation law

(1). Already done

(2). Already done

(3). Let G be finite group

Suppose $(ab)^3 = a^3 b^3 \quad \forall a, b \in G$

$(ab)^3 = a^3 b^3$

$(ab)(ab)(ab) = a^3 b^3$

Scanned with CamScanner

(Cancellation)

$(ba)(ba) = a^2 b^2$
$(ba)^2 = a^2 b$

$(ba)^3 = b^2 a^3$
$ba(ba)^2 = b^3 a^3$
$a^3 b^2 = b^2 a^3$

And every element of g can be uniquely represented as cube

$a^2 b^2 = b^2 a^2$
$(ba)(ba) = b^2 a^2$
$ab = ba$ Proved.

④. P.T any subgrop of a cyclic group is a cyclic group.

Let $G = [a]$ be cyclic grp
H is a subgrp of G.

If $H = G$ or $H = \{e\}$,
H is also a cyclic group.

If H is proper subgroup, H contains one element a^m other than e
$a^m \in H \rightarrow a^{-m} \in H$

Let m be least +ve integer, $\forall a^m \in H$
Let $a^n \in H \rightarrow$ division algorithm
there exists two integers q, r.
$n = mq + r$ $\quad 0 \leq r < m$
$n - mq = r$

Since
$a^m \in H \rightarrow (a^m)^q \in H$

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

Now $a^n \in H$,
$a^{-mq} \in H$
$a^{n-mq} \in H$
$a^r \in H \rightarrow n-mq = r$

But since m is least +ve,
$r = 0$

So, $a^n = a^{mq}$
$a^n = (a^m)^q$
$H = [a^m]$.

Every subgroup of G is cycleric.

Q.5) How many generators a cyclic group of order n can have?

When the order of cyclic group is n, there will be 'one' generator for every number between 1 n that is relatively prime to n.

Example:- $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$\langle 0 \rangle = \{0\}$
$\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 0\}$
$\langle 2 \rangle = \{2, 4, 6, 0\}$
$\langle 3 \rangle = \{3, 6, 1, 4, 7, 2, 5, 0\}$
$\langle 4 \rangle = \{0, 4\}$
$\langle 5 \rangle = Z_8$
$\langle 6 \rangle = \{0, 2, 4, 6\}$
$\langle 7 \rangle = Z_8$

$\therefore P(n) = 4 \Rightarrow$ no. of relatively Prime to 8.

Q.6) If $a \in G$ & a^m & $= e$, P.T. $O(a)/m$.

Given that $a^m = e$. $a \in G$.

$\Rightarrow$ a has finite order $\Rightarrow K = O(a)$.

By the division algorithm, there exists unique integers r, q, &

$m = kq + r$

Now, $e = a^m = a^{kq+r} \Rightarrow a^{kq} \cdot a^r = (a^k)^q a^r$

$= e^q a^r = a^r$

But since k is the smallest positive integer possible, $r = 0$

$m = kq + r = kq + 0$

$\frac{m}{k} = q$

$\frac{m}{o(a)} = q$

$\therefore$ order of a divides m.

Q.7) If G has no non trivial subgroups. S.T. G must be finite of prime order.

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

Since it has no non-trivial sub-groups, there only G and $\{e\}$ are its sub groups where e is identity.

Now, by Lagranges theorum, $O(G) = k\, O(H)$

$\Rightarrow$ order of group G is divisible by order of sub groups H.

Since the subgroups are G and $\{e\}$ their orders are n and 1.

So, n has only two factors = n and 1.

this means n is a prime number.

U19CS076

$\therefore$ G must be Primitive of Prime order.

Q.8) Let G be group that the intersection of all its sub group which are different from (e) is a sub group and different from identity. Prove that every element in G has finite order.

Let $\cap\{e\} \neq H \leq G$. $H = K \neq \{e\}$.

Let $H_i = \langle a^i \rangle$ are sub-groups of G.

since $K \leq N$

($\because$ Subgroup of cyclic group)

= for some integer n

Since $\langle a^n \rangle \leq \langle a^i \rangle$

$n = iK$ i_H i/n

As n is a fixed given Positive no it has only finitely many divisions. Since $K \neq e$, we only have finitely many $H_i \neq e$ i.e. There exists a j such that $H_j = \langle a^i \rangle = e$ i.e. $a^j = e$.