Abstract Algebra

[Handwritten Study Material with solved examples]

[For NET, GATE, SET, JAM, NBHM, PSC, MSc, ...etc.]

✍
P. Kalika
(NET(JRF), GATE, SET)
Email: maths.whisperer@gmail.com

No. of Pages: 50

Content:

4.5

Page No. 183

SYLOW'S THEOREM

Def?— let G be a group & let p be a prime.

(1) A group of order p^α for some $\alpha \geq 1$ is called as p-group. A subgroup of G is called p-subgp.

(2) If G is a group of order $p^\alpha m$ where $p \nmid m$ then a subgroup of order p^α is called a Sylow p-subgroup of G.

(3) $Syl_p(G)$ = Set of sylow p-subgps of G
$n_p(G)$ = no. of sylow p-subgps of G.

Theorem (18)

SYLOW'S THEOREMS:—

(i) Sylow Theorem 1: let G be a group of order $p^\alpha m$ where p is a prime not dividing m i.e $p \nmid m$. Then $\exists$ a sylow p-subgp of G of order p^α, i.e

$$Syl_p(G) \neq \phi$$

(ii) Sylow theorem 2: If P is a sylow p-subgp of G & Q is any p-subgrp of G, then $\exists$s $g \in G$ s.t $Q \subseteq gPg^{-1}$ i.e Q is contained in some conjugate of P.

In particular, Any two sylow p-subgps are conjugate in G.

(iii) Sylow theorem 3: The no. of distinct sylow p-subgps divides $|G|$ & is of the form $kp+1$

i.e $n_p = kp+1$

or $n_p \equiv 1 \mod p$

i.e $n_p = |G : N_G(P)|$

Page No. 184
Date.

Corollary (20): A sylow p-subgp is normal iff it is unique.

Pf: (1) let G be a gp of order $p^\alpha m$ s.t $p \nmid m$
let P be a sylow p-subgp of G then
$$|P| = p^\alpha$$

Given: —

Sylow p-subgp is unique.
Now for $g \in G$, $gPg^{-1} \leq G$
& $|gPg^{-1}| = |P| = p^\alpha$
$\Rightarrow$ gPg^{-1} is also a sylow p-subgp of G.

as there is only one sylow p-subgp of G.
$\Rightarrow$ $gPg^{-1} = P$ $\forall g \in G$.
$\Rightarrow$ $P \triangle G$.

$\Leftarrow$ let $P \triangle G$.
T.P P is unique.
let Q be any other sylow p-subgroup of G then by sylow theorem 2 $\exists$
$\exists$ $g \in G$ s.t $Q = gPg^{-1}$
&
$Q = gPg^{-1} = P$ $\forall g \in G$.
$\because$ $P \triangle G$.
$\Rightarrow$ $Q = P$
$\Rightarrow$ Sylow p-subgp is unique.

(2) P is normal in G $\Leftrightarrow$ All subgps generated by elts of p-power order are p-groups
i.e if X is any subset of G s.t $|x| =$ Power of p $\forall x \in X$ then $\langle x \rangle$ is a p-group.

Pf: let X be any subset of G s.t
$|x| =$ Power of p $\forall x \in X$.

Page No. 185

Then by Sylow thm-2, for each $x \in X$. $\exists g \in G$ s.t $x \in gPg^{-1} = P$ $\because P \Delta G$

$\Rightarrow x \subseteq P$

$\Rightarrow \langle x \rangle \le P$ & $\langle x \rangle$ is a P-group.

$\Leftarrow$ let $\langle x \rangle$ is a p-group.

let X be the union of all sylow p-subgps of G.

P is a sylow p-subgps of G.

$\Rightarrow p \subseteq \langle x \rangle$

Since, P is a p-subgp of G of maximal order

$\Rightarrow \langle x \rangle = P$

$\Rightarrow P$ is the unique sylow-subgp. $P \Delta G$.

APPLICATION OF 'SYLOW' THRM

Theorem: (24-7) 2014 If $|G| = pq$ with p & q primes with $p<q$ & $p \nmid (q-1)$ then G is cyclic.

Pf: As $p<q$ & $p \nmid q-1$

$\Rightarrow q \nmid p-1$

Now, $|G| = pq \Rightarrow p \mid |G|$ but $p^2 \nmid |G|$

$\therefore G$ has sylow p-subgps of order p.

$\therefore$ By Sylow theorem —

No. of distinct sylow p-subgp is of the form $1+kp$, $(k \ge 0)$

i.e $n_p = 1+kp$

$\Rightarrow 1+kp \mid |G| \Rightarrow 1+kp \mid pq$

As $(1+kp, p) = 1 \Rightarrow 1+kp \mid q$

$\Rightarrow 1+kp = 1$ or q

Now, $1+kp = 1 \Rightarrow k=0$ or $1+kp = q$

$\Rightarrow kp = q-1 \Rightarrow p \mid q-1$

not possible (given)

Page No. 186
Date

$1+kp=1 \Rightarrow k=0$

$\Rightarrow \exists$ only one sylow p-subgp of G say P.

$|P| = p$

$||^{ly}$ $\exists$ only one sylow q-subgp of G say Q.

$|Q| = q$

As P is the unique sylow p- subgp of G. $\Rightarrow P \Delta G$.

$||^{ly}$ Q is the unique sylow q-subgp of G $\Rightarrow Q \Delta G$.

We'll now, show that $P \cap Q = \{e\}$

Now, $P \cap Q \subseteq P$ & $P \cap Q \subseteq Q$

$\Rightarrow |P \cap Q| \, / \, |P|$ & $|P \cap Q| \mid |Q|$

$\Rightarrow |P \cap Q| \mid p$ & $|P \cap Q| \mid q$ as $(p, q) = 1$

$\Rightarrow |P \cap Q| = 1$

$\Rightarrow P \cap Q = \{e\}$

Now,

$|P| = p \Rightarrow P$ is cyclic

$|Q| = q \Rightarrow Q$ is cyclic.

[Every gp of prime order is cyclic

Let $P = \langle x \rangle$ for $x, y \in G$

$Q = \langle y \rangle$, $|x| = p$, $|y| = q$

We'll prove that x & y commute.

Consider, $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Q \quad \because Q \Delta G$

$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in P \quad \because P \Delta G$.

$\Rightarrow xyx^{-1}y^{-1} \in P \cap Q = \{e\}$

$\Rightarrow xyx^{-1}y^{-1} = e \Rightarrow xy = yx$

$\Rightarrow |xy| = |x||y| = pq = |G|$ [$\because xy = yx$, $|xy| = |x||y|$)

$\Rightarrow G = \langle xy \rangle \Rightarrow G$ is a cyclic gp generated by xy.

Page No. 187

and as G is a cyclic gp of order pq.
$\Rightarrow G \simeq \mathbb{Z}_{pq}$.

Que Prove that every gp of order 15 is cyclic.

$|G| = 15 = 3 \cdot 5$ $\quad p=3, \; p<q$
$3 \nmid 4$ $\quad q=5, \; \& \; p \nmid q-1$

$\Rightarrow$ by above thm, G is cyclic.

(wi) Que Prove that if $|G| = p^2q$ where p & q are distinct primes with $p>q$ then G has a normal subgroup of order p^2.

$|G| = p^2q$
$\Rightarrow p^2 \mid |G|$
$\therefore$ Sylow p-subgps are of order p^2.
n_p = No. of distinct sylow p-subgps that divides $|G|$
$\Rightarrow n_p = kp+1 \mid |G| \quad k \geq 0$
$\therefore kp+1 \mid p^2q$
Now,
$(kp+1, p^2) = 1$
$\Rightarrow (kp+1) \mid q$.
Now, if $k \geq 1$ then $kp \geq p$
$\therefore kp+1 > p > q$
$\Rightarrow kp+1$ can't divide q if $k \neq 0$.
i.e $k=0 \; \therefore n_p = 1$
Thus $\exists$ a unique sylow p-subgp say P of order p^2 s.t $P \triangle G$.

Case-II If $|G| = p^2q$ where p & q are distinct prime with $p<q$. P.T then G has a normal subgp of order q or $|G| = 12$.

Page No. 188
Date

Solⁿ. as $|G| = p^2q$

$\therefore$ G can have a sylow p-subgrp of order q.

$n_q = kq+1$ is the no. of distinct sylow q-subgroups of G.

$\Rightarrow (kq+1) \mid |G| \Rightarrow (kq+1) \mid p^2q$

As $(kq+1, q) = 1 \Rightarrow (kq+1) \mid p^2$

$\Rightarrow kq+1 = 1$ or p or p^2

(i) $kq+1 = 1 \therefore k=0 \Rightarrow \exists$ a unique sylow q-subgrp of order q say Q. $|Q| = q$.

$\Rightarrow \boxed{Q \Delta G}$ $\because$ Q is unique.

(ii) $kq+1 = p < q$ not possible $(p<q)$

(iii) $kq+1 = p^2$

$\therefore kq = p^2 - 1 = (p-1)(p+1)$

$\therefore q \mid (p-1)(p+1) \quad \therefore q \mid p-1$ or $q \mid p+1$

As $q > p \Rightarrow q \nmid p-1$

$\therefore q \mid p+1$

As, $q > p \Rightarrow q \geq p+1$ } $q = p+1$ consecutive prime

$\therefore p = 2$ & $q = 3$

$\Rightarrow |G| = p^2q = 12$.

Que. Show that a group of order 30 has normal subgroup of order 15. (i.e isomorphic to Z_{15})

Sol:- $|G| = 30 = 2 \cdot 3 \cdot 5$

$\Rightarrow 3 \mid |G| \quad \therefore$ G has sylow 3 subgps of order 3.

$\Rightarrow n_3 =$ No. of distinct sylow 3-subgps divides $|G|$.

$\Rightarrow 3k+1 \mid |G| \quad , k \geq 0$

$\Rightarrow 3k+1 \mid 2\cdot 3\cdot 5$

$(3k+1, 3) = 1 \Rightarrow (3k+1) \mid 10$

$\therefore 3k+1 = 1$ or 2 or 5 or 10.

$3k+1 = 1 \Rightarrow k = 0$

$3k+1 = 2 \Rightarrow k = 1/3$ not possible.

$3k+1 = 5 \Rightarrow k = \frac{4}{3}$ " "

$3k+1 = 10 \Rightarrow k = 3$

$\Rightarrow$ There is either one or 10 distinct sylow 3-subgps.

i.e $n_3 = 1$ or 10

||^{ly} $n_5 = 1$ or 6

$(5k+1) \mid 6 \Rightarrow 5k+1$ or 2 or 3 or 6

$\Rightarrow 5k+1 = 1 \Rightarrow k = 0$

$5k+1 = 6 \Rightarrow k = 1$

If possible suppose $n_3 = 10$ & $n_5 = 6$.

$\Rightarrow \exists$ 10 distinct sylow 3-subgroups. $P_1, P_2, \ldots P_{10}$

$\exists$ 6 ——— 5-subgps, $Q_1, Q_2, \ldots Q_6$.

$\because |P_i| = 3 \Rightarrow$ Every non-identity elt. of P_i is of order 3. There are 2 non-identity elts in each P_i, $i = 1, 2, \ldots, 10$.

$\Rightarrow$ No. of distinct elt.s of order $3 = 10 \times 2 = 20$

||^{ry} ——— $5 = 6 \times 4 = 24$.

Total $= 20 + 24 = 44$ elts

$\Rightarrow |G| > 30$

Not Possible.

$\Rightarrow n_3 \neq 10$ & $n_5 \neq 6$

$\Rightarrow n_3 = 1$ or $n_5 = 1$

$\Rightarrow \exists$ a unique sylow 3-subgp say P.

$\exists$ a unique sylow 5-subgps say Q.

Page No. 190
Date

$\Rightarrow P \Delta G$ & $Q \Delta G$.

As $\boxed{P \Delta G \text{ \& } Q < G \Rightarrow PQ < G}$

Also, $|PQ| = \dfrac{|P||Q|}{|P \cap Q|} = \dfrac{3 \cdot 5}{1} = 15$

$\boxed{P \cap Q = \{e\}}$

$|G : PQ| = \dfrac{30}{15} = 2$

$\therefore PQ \Delta G$ [Every subgp. of index 2 is normal in G]

$|PQ| = 15$ - cyclic

$\approx Z_{15}$

* Index Theorem :

If G is a finite group & H is a proper subgroup of G s.t $|G|$ doesn't divide $|G:H|!$ then H contains a non-trivial normal subgp of G. In particular, G is not simple.

Result:- 2-odd Test:— An integer of the form $2 \cdot n$ where n is an odd no. greater than 1. is not the order of a simple group.

Que: Prove that a gp. of order 56 has a normal sylow p-subgp for prime p dividing its order.

(CH-24 Q-12)

Sol^n:- $|G| = 56 = 2^3 \cdot 7$

Then G has sylow 2-subgps of order $2^3 = 8$

G has sylow 7-subgps of order $= 7$

n_7 = No. of distinct sylow 7-subgp of order 7 that divides $|G|$.

$\Rightarrow (7K+1) \mid |G|$, $K \geq 0$

$\Rightarrow (7K+1) \mid 2^3 \cdot 7$

Page No. 191
Date

or $\left((7k+1), 7\right) = 1$

$\Rightarrow (7k+1) \mid 2^3$

$\Rightarrow (7k+1) \mid 8 \Rightarrow 7k+1 = 1$ or 2 or 4 or 8

$\Rightarrow 7k+1 \neq 2$ or 4

$\Rightarrow 7k+1 = 1$ or $7k+1 = 8$ $\boxed{n_7 = 1 \text{ or } 8}$

$\Rightarrow k = 0$ or 1

n_2 = No. of distinct sylow 2-subgrps of order 8

$\Rightarrow (2k+1) \mid |u| \Rightarrow (2k+1) \mid 2^3 \cdot 7$

$\Rightarrow (2k+1, 8) = 1$

$\Rightarrow (2k+1) \mid 7$

$\Rightarrow 2k+1 = 1$ or 7.

$\Rightarrow k = 0$ or $k = 3$.

$\Rightarrow \boxed{n_2 = 1 \text{ or } 7}$

We ~~have~~ Prove that $n_2 \neq 7$ & $n_7 \neq 8$

if $n_2 = 7$ & $n_7 = 8$,

There are 7-Sylow 2-Subgrps say $H_1, H_2, \cdots, H_7$

—— 8-sylow 7-subgrps —— $K_1, K_2, \cdots, K_8$

As all ~~the~~ are distinct &

$|H_i| = 8$, $|K_i| = 7$

$|K_i| = 7 \Rightarrow$ there are 6 non-identity elts of order 7.

$\Rightarrow$ No. of elts of order $7 = 8 \times 6 = 48$

Consider H_i,

if $x \in H_i$, $1 \le i \le 7$.

then $|x| = 2^\alpha$, $0 \le \alpha \le 3$, $\because |H_i| = 2^3$.

Consider $H_1 \cap H_2$, Since $H_1 \neq H_2$

$\Rightarrow |H_1 \cap H_2| = 2^\beta$, $0 \le \beta \le 2$

$|H_1 \cup H_2| = |H_1| + |H_2| - |H_1 \cap H_2|$

$= 2^3 + 2^3 - 2^\beta$

$= 16 - 2^\beta \ge 12$

Page No. 192
Date

$\Rightarrow$ G has at least 12 elt.s of order in power of 2.
$\Rightarrow$ G has at least $12+48=60$ non-identity elt.s.

But $|G| = 56 < 60$ Contradiction
$\Rightarrow n_2 \neq 7$ or $n_7 = 8$
$\Rightarrow$ G has either one sylow 2-subgp of or has only 1 sylow 7 subgp.

$\Rightarrow$ G is not simple
as $n_2 = 1$ or $n_7 = 1$
$\Rightarrow$ it has a unique sylow 2-subgp P (say)
$\therefore P \Delta G$.
or it has a unique sylow 7-subgp Q (say)
$\Rightarrow Q \Delta G$.

(W)
Que-17 $|G| = 105$. Then G has a normal sylow 5-subgp & a normal sylow 7-subgp.
(Ex-4.5)
Sol^n:- $|G| = 105 = 3 \cdot 5 \cdot 7$
It has sylow 3-subgps of order 3.
——— 5 - ——— 5
——— 7 - ——— 7

n_5 = No. of distinct sylow 5-subgps of order 5.
n_7 = No. of distinct sylow 7-subgps of order 7

$\Rightarrow n_5 = (5k+1) \mid |G|$
$n_7 = (7k+1) \mid |G|$

$\Rightarrow (5k+1) \mid 3 \cdot 5 \cdot 7$ as $(5k+1, 5) = 1$
$\Rightarrow (5k+1) \mid 3 \cdot 7 = 21$
IIIy $(7k+1) \mid 15$

$\Rightarrow 5k+1 = 1$ or 3 or 7 or 21

$5k+1 \neq 3$ & 7

$\Rightarrow 5k+1 = 1$ or 21

|||ly $7k+1 = 1$ or 15

Now $n_7 = 1$ or 15, $n_5 = 1$ or 21

If $n_7 = 15$, & $n_5 = 21$

$\Rightarrow \exists$ 15 distinct sylow 7-subgroups $H_1, H_2, ---, H_{15}$

$\exists$ 21 distinct sylow 5-subgroups $K_1, K_2, ---\ K_{21}$

$\Rightarrow |H_i| = 7$ & $|K_i| = 5$

Every H_i has 6 non-identity elts of order 7
Every K_i has 4 non-identity elts of order 5.

$\exists$ $6 \times 15 = 90$ elts of order 7.

& $\exists$ $4 \times 21 = 84$ ——— 5

$\Rightarrow 90 + 84 = 174$ elts of G.
not possible.

$\Rightarrow$ Either $n_5 = 1$ or $n_7 = 1$

<u>If $n_5 = 1$</u>

$\Rightarrow \exists$ a unique sylow 5-subgps of order 5 say P.

$\exists$ a unique sylow 7-subgp of order 7 say Q.

Now,

$P \trianglelefteq G$ & $Q < G$, $P \cap Q = \{e\}$

Then $PQ < G$

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{5 \cdot 7}{1} = 35$$

$$|G : PQ| = \frac{105}{35} = 3$$

Page No. 194
Date

$PQ \Delta H$

Now $P \Delta H$ & $PQ \Delta H \Rightarrow Q \Delta H$
ll'ry for $n_7 = 1$.

(Ex-405)
Que (6) Exhibit all sylow 3-subgps of S_4 & all sylow 3-subgps of A_4.
(Un-24 Ex-8)

Sol^n

$|S_4| = 24 = 2^3 \cdot 3$

$|A_4| = 12 = 2^2 \cdot 3$

A_4 & S_4 has sylow 3-subgroups of order 3

In A_4:-

$n_3 = 3k+1$ = no. of distinct sylow 3-subgp of order 3.

$(3k+1) | 12 \Rightarrow (3k+1) | 4 \cdot 3$
$\Rightarrow (3k+1) | 4$
$\Rightarrow 3k+1 = 1$ or 4
$n_3 = 1$ or 4.

There can be 4 sylow 3-subgps of order 3.

$A_4 = \{ I, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (14)(23), (13)(24) \}$

$\langle (123) \rangle = \{ I, (123), (132) \}$
$\langle (124) \rangle = \{ I, (124), (142) \}$
$\langle (134) \rangle = \{ I, (134), (143) \}$
$\langle (234) \rangle = \{ I, (234), (243) \}$

All 4 sylow 3-subgps of A_4.

In S_4: $n_3 = 1$ or 4 or 8
but $3k+1 \neq 8$ $\because k = 7/3$ not possible
S_4 has 4, sylow 3-subgps of order 3.
(same as A_4).

Page No. 195

Date

* A_4 has a unique sylow 2 subgrp.

$$|A_4| = 12 = 2^2 \cdot 3$$

$n_2 = 2k+1$ are distinct sylow 2-subgrps

$(2k+1) \mid 3 \Rightarrow 2k+1 = 1$ or 3.

$2k+1 = 1 \Rightarrow k = 0$ | $2k+1 = 3 \Rightarrow k = 1$

Let P be the sylow 2-subgroup of A_4 of order '4'.

$P = \{I, (12)(34), (13)(24), (14)(23)\}$

$\Rightarrow P \Delta A_4$. Hence unique.

(Ex-4.5)

Que: Exhibit all sylow 2-subgps of S_4.

(Ch-24, Ex-5)

$$|S_4| = 24 = 2^3 \cdot 3$$

$n_2 = 2k+1 =$ no. of distinct sylow 2-~~group~~ subgrp of order 8

$(2k+1) \mid |S_4| \Rightarrow (2k+1) \mid 2^3 \cdot 3$

$\Rightarrow (2k+1) \mid 3$

$\Rightarrow 2k+1 = 1$ or 3

$n_2 = 3$

Let P_1, P_2, P_3 be sylow 2-subgroups of order 8.

Since S_4 contains a subgroup of S_4 is isomorphic to D_8.

* * *

Section-II ENDS

Section-2

* * *

Chapter-3 (3.4) (Dummit & Foote)

COMPOSITION SERIES AND THE HOLDER PROGRAMME :—

Lemma (21): If G is a finite abelian grp & p is a prime dividing $|G|$, then G contains an elt. of order p.

Pf: let p be a prime dividing $|G|$.

$|G| \geq 2$.

(i) If $|G| = 2$
Then G contains an elt. of order 2.
$x \in G$, $x \neq e$, s.t $x^2 = e$.

(ii) Now, let us assume that result is true for all grps. with order less than $|G|$. i.e for any grp. whose order is less than $|G|$ of p divides its order then $\exists$ an elt. of order p.

Case-I, If G has no proper subgrp. then $o(G)$ is Prime.
$\Rightarrow p \mid |G| \Rightarrow p = |G|$
Then G is a cyclic grp.
$\Rightarrow \exists\ x \in G$ s.t $x^p = e$ $(x \neq e)$

Case-II, let G has a proper subgrp. H.

Then $H \neq \{e\}$ & $H \neq G$

If $p \mid |H|$ where $H < G \Rightarrow |H| \mid |G|$
& $|H| \mid |G|$

& by our assumption result is true for H.

$\Rightarrow \exists$ an elt. other than identity in H. i.e
$e \neq a \in H \Rightarrow a^p = e$.

If $p \nmid |H|$, then G is abelian &
$H \leq G$. $\Rightarrow H \triangleleft G$ & G/H is defined
& in an abelian group.

Also, $\left|\frac{G}{H}\right| = \frac{|G|}{|H|} < |G|$. Now, $p \mid |G|$
& $p \nmid |H| \Rightarrow p \mid \left|\frac{G}{H}\right|$

Then,
by our assumption result is true for $\frac{G}{H}$.
$\therefore \exists$ an elt. $bH \in \frac{G}{H}$ $(bH \neq H)$
s.t $(bH)^p = H$
$\Rightarrow b^pH = H \Rightarrow b^p \in H$
$\Rightarrow (b^p)^{|H|} = e \Rightarrow (b^{|H|})^p = e$
$\Rightarrow a^p = e$ where $b^{|H|} = a \in G$.

We claim that $a \neq e$
if $a = e \Rightarrow b^{|H|} = e$
$\Rightarrow (bH)^{|H|} = b^{|H|}H = H$
$\Rightarrow |bH| \mid |H| \Rightarrow p \mid |H|$ — Contradiction

$\Rightarrow a \neq e$ & $a^p = e$.

Defn: **Simple Group :—**

A finite or Infinite grp is called simple if $|G| > 1$ & the only normal subgrp of G are $\{e\}$ & G.

Page No. 256
Date

Note:- Every grp of prime order is simple.

Pf: let G be a grp of prime order.
$|G| = p$
Let $H \leq G$
Then $|H| \mid p \Rightarrow |H| = 1$ or p
$\Rightarrow H = \{e\}$ or $H = G$
$\therefore$ G is a simple group.

Def^n: **Composition Series :-**
In a group G, a sequence of subgrps.
$\{e\} = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{K-1} \leq N_K = G$
is called a Composition Series if

$$N_i \triangle N_{i+1} \ \& \ \frac{N_{i+1}}{N_i} \text{ is a simple grp.}$$

for $0 \leq i \leq k-1$
The quotient grp $\frac{N_{i+1}}{N_i}$ is called composition factors of G.

Ex- $D_4 = \{1, r, r^2, r^3, s, rs, r^2s, sr^3 \mid r^4 = 1 = s^2, rs = s^{-1}r\}$

$\langle s \rangle = \{1, s\}$
$\langle s, r^2 \rangle = \{1, s, r^2, sr^2\}$
Here $\{1\} \triangle \langle s \rangle \triangle \langle s, r^2 \rangle \triangle D_4$
$\{1\} \triangle \langle r^2 \rangle \triangle \langle r \rangle < D_4$
There are 2 composition series for D_4.

Que: Obtain the Composition series of Q_8.
Ex - Q.2

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

$i^2 = -1 = (-i)^2$ $\quad$ $i.j = k = -j.i$
$j^2 = -1 = (-j)^2$ $\quad$ $j.k = i = -k.j$
$k^2 = -1 = (-k)^2$ $\quad$ $k.i = j = -i.k$

Consider —

$N_0 = \{1\}$

$N_1 = \{1, -1\}$

$N_2 = \{1, -1, i, -i\}$

$N_3 = Q_8$

$\boxed{\{1\} = N_0 \leq N_1 \leq N_2 \leq N_3 = Q_8}$ & $N_0 \Delta N_1$, $N_1 \Delta N_2$, $N_2 \Delta N_3$

$\frac{N_1}{N_0}, \frac{N_2}{N_1}, \frac{N_3}{N_2}$ are simple gps

(2) $N_0 = \{1\}$
$N_1 = \{1, -1\}$
$N_2 = \{1, -1, j, -j\}$
$N_3 = Q_8$

(3) $N_0 = \{1\}$
$N_1 = \{1, -1\}$
$N_2 = \{1, -1, k, -k\}$
$N_3 = Q_8$.

Que. Give an example of an infinite gp which has no composition series.

Pf:- Consider $(\mathbb{Z}, +)$

let if possible $\mathbb{Z}$ has a composition series.

let $\{0\} = N_0 \leq N_1 \leq \ldots\ldots \leq N_k = \mathbb{Z}$ be the composition series for $\mathbb{Z}$. s.t

$N_i \Delta N_{i+1}$ & $\frac{N_{i+1}}{N_i}$ is ~~prime~~. Simple.

Now, $\left|\frac{N_1}{N_0}\right| = |N_1|$

$\Rightarrow \frac{N_1}{N_0} \approx N_1$ as $\frac{N_1}{N_0}$ is simple.

$\Rightarrow N_1$ is also simple.

$\Rightarrow N_1$ has only 2 normal subgps $\{0\}$ & N_1 itself.

Now as N_1 is a subgp of $\mathbb{Z}$ & $\mathbb{Z}$ is cyclic.

$\Rightarrow N_1$ is also cyclic.

let $N_1 = \langle k \rangle$ f.s $k \in \mathbb{Z}$

Then $H = \langle 2k \rangle$ is a normal subgp of N_1

$H \neq N_1 \Rightarrow$ Contradiction as N_1 is simple.

Page No. 158
Date

Thm (22)

JORDAN - HOLDER THM :— (Thm-22)

let G be a finite group with $G \neq \{e\}$. Then

(i) G has a composition series &

(ii) The composition factors in a composition series are unique, namely if -

$$\{e\} = N_0 \leq N_1 \leq N_2 - \leq N_r = G$$

$$\{e\} = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_s = G$$

(Pf not required)

are 2 composition series for G then $r = s$ & for every $1 \leq i \leq r-1$, $\exists$ j s.t

$$\frac{M_{j+1}}{M_j} \approx \frac{N_{i+1}}{N_i}$$

Def: **Solvable Groups :—**

A grp G is solvable if there is a chain of subgrps.

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \cdots \trianglelefteq G_s = G$$

s.t $\frac{G_{i+1}}{G_i}$ is an abelian group for $i = 0, 1, 2, \cdots s-1$

Result: Show that every abelian grp. is solvable.

Sol^n- let G be an abelian grp.

Consider $G_0 = \{e\}$, $G_1 = G$

$\{e\} \trianglelefteq G$

Also, $\left|\frac{G_1}{G_0}\right| = \frac{|G_1|}{|G_0|} = |G|$ $\therefore \frac{G_1}{G_0} \approx G$.

Since G is abelian $\Rightarrow \frac{G_1}{G_0}$ is Abelian

$\Rightarrow G$ is solvable.

Result: Every cyclic grp. is solvable.

Result: let G be a non-abelian simple group. Show that G is not - solvable.

Page No. 159
Date

Pf:— As G is a simple grp.
$\therefore$ the only normal subgrps are $\{e\}$ & G.
Also, $\frac{G}{\{e\}} \approx G$. As G is non-Abelian.
$\Rightarrow \frac{G}{\{e\}}$ is non-Abelian.
$\Rightarrow G$ is not solvable.

Cor. A_5 is not solvable. ($\because A_5$ is a non-Abelian simple-grp)

Que-1 Show that S_3 & S_4 are solvable.

We know that $I \leq A_3 \leq S_3$

Also, $I \triangle A_3$ & $A_3 \triangle S_3$.

$$\left|\frac{S_3}{A_3}\right| = 2 = \text{Prime}$$

Every group of Prime order is cyclic. Hence abelian.

$|||^{ly}$ $\left|\frac{A_3}{I}\right| = 3 = \text{Prime} \Rightarrow \frac{A_3}{I}$ is also abelian.

$\Rightarrow S_3$ is solvable.

$|||^{ly}$, Consider $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

$I \triangle K_4 \triangle A_4 \triangle S_4$

$\left|\frac{S_4}{A_4}\right| = \frac{24}{12} = 2 = \text{Prime}$. Hence $\frac{S_4}{A_4}$ is abelian.

$\left|\frac{A_4}{K_4}\right| = \frac{12}{4} = 3 = \text{Prime}$. Hence $\frac{A_4}{K_4}$ is abelian.

$\left|\frac{K_4}{I}\right| = 4 = 2^2$ — every grp of order p^2 is abelian

$\Rightarrow \frac{K_4}{I}$ is abelian.

$\Rightarrow S_4$ is solvable.

Page No. 160

Que: 7 (Ex-3.4) Prove that if G is an abelian simple gp. then $G \approx Z_p$ for some prime p.

Pf: As G is abelian $\Rightarrow$ All its subgps are normal.
But as G is simple.
$\Rightarrow$ There are only 2 normal subgps of G.
$\{e\}$ & G itself.
But we know that if G is infinite then all distinct elts will generate a subgp.
$\Rightarrow$ G can't be infinite.
$\Rightarrow$ G must be finite.
$\therefore$ By ~~converges~~ converse of Lagrange's thm — for finite abelian group. if $|G| =$ is not a prime then it will have subgps which is a contradiction as G has only 2 normal subgps.
$\Rightarrow$ $|G| = p$ $\Rightarrow$ G is cyclic gp of order p.
$\Rightarrow$ $G \approx Z_p$.

Que-8 (Ex-3.4) Prove that subgps & Quotient of a solvable gp are solvable.

Pf: To prove this Result, we have to prove
Let G be a group. &
$x^{-1}y^{-1}xy$ is a commutator in G.
& $G' =$ subgp generated by $\{x^{-1}y^{-1}xy : x, y \in G\}$
Every elt. of G' is of the form

$p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}$ where each p_k is a commutator

Then G' is called a commutator subgp of G.
Also $G' \trianglelefteq G$ & G' is the smallest normal subgp s.t $\frac{G}{G'}$ is abelian if $N \trianglelefteq G$ s.t $\frac{G}{N}$ is abelian then—

$G' \subseteq N$ —— $(*)$

Page No. 161
Date

Theorem (Ch-6, Thm-9) A Group G is solvable iff $G^{(n)} = \{e\}$ for some +'ve integer n where $G^{(n)}$ is the n^{th} commutator subgrp of G.

$$G^{(2)} = (G')'$$
$$G^{(3)} = (G^{(2)})'$$

pf: let G be a solvable then, $\exists$ series say $\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n = G$ where each $G_i \Delta G_{i+1}$ & $\frac{G_{i+1}}{G_i}$ is abelian.

Now, $\frac{G_n}{G_{n-1}}$ is abelian i.e $\frac{G}{G_{n-1}}$ is abelian & $G_{n-1} \Delta G$

Then $\boxed{G' \subseteq G_{n-1}}$ by $(*)$

$\Rightarrow (G')' \subseteq G'_{n-1} \Rightarrow G^{(2)} \subseteq G'_{n-1}$

Again $\frac{G_{n-1}}{G_{n-2}}$ is Abelian & $G_{n-2} \Delta G_{n-1}$

$\Rightarrow G'_{n-1} \subseteq G_{n-2}$

$\Rightarrow G^{(2)} \subseteq G_{n-2}$

||'rly $G^{(3)} \subseteq G_{n-3}$

$G^{(n)} \subseteq G_0 = \{e\} \Rightarrow G^{(n)} = \{e\}$.

$\Leftarrow$ Suppose, $G^{(n)} = \{e\}$ f.s +ve integer 'n'.

Consider the series $G' \subseteq G \Rightarrow (G')' \subseteq G'$

$\Rightarrow G^{(2)} \subseteq G^{(1)}$

$\Rightarrow (G^{(2)})' \subseteq (G')'$

$\Rightarrow G^{(3)} \subseteq G^{(2)}$

$\Rightarrow \{e\} = G^{(n)} \subseteq G^{(n-1)} \subseteq \dots \subseteq G' \subseteq G$.

As, $G' \Delta G \Rightarrow G^{(i)} \Delta G^{(i-1)}$

$\Rightarrow \frac{G^{(i-1)}}{G^{(i)}}$ is abelian.

$\Rightarrow G$ is solvable.

Page No. 162

Every subgroup of a solvable grp is solvable.

Pf: let H be a subgroup of a solvable group G.
Since G is solvable
$\Rightarrow G^{(n)} = \{e\}$ f.s $n \in \mathbb{N}$
as $H \subseteq G \Rightarrow H' \subseteq G' \Rightarrow (H')' \subseteq (G')'$
$\Rightarrow H^{(n)} \subseteq G^{(n)} = \{e\}$
$\Rightarrow H^{(n)} = \{e\} \Rightarrow H$ is solvable.

Result: Quotient group of a solvable grp. is solvable.

Pf: let G be a solvable grp. & $H \Delta G$. Then $\frac{G}{H}$ is a quotient grp.
Define $\phi : G \to G/H$ as $\phi(g) = gH \ \forall g \in G$.
ϕ is an onto H.M
$\Rightarrow$ As Homomorphic image of a solvable grp is solvable.
$\Rightarrow \frac{G}{H}$ is also solvable.

Theorem A simple Group is solvable iff G is Abelian.

Pf: If G is Abelian & simple $\Rightarrow G$ is solvable

$\Leftarrow$ Let G be simple and solvable.
As $G' \Delta G$ & G is simple.
$\therefore G' = \{e\}$ or $G' = G$
As G is solvable by lemma
$G' \neq G$
(Ex 3.4) $\therefore G' = \{e\} \Rightarrow G$ is Abelian

$x^{-1}y^{-1}xy \in G' = \{e\}$
$\Rightarrow x^{-1}y^{-1}xy = \{e\}$
$\Rightarrow xy = yx$
$\Rightarrow G$ is Abelian

Q.8

Theorem let G be a finite group. Show that G is solvable iff $\exists$ a series of subgroups. $\{e\} = H_0 \Delta H_1 \Delta \cdots \Delta H_n = G$ s.t $\frac{H_{i+1}}{H_i}$ is cyclic.

Let G be solvable. Since G is finite

$\therefore$ it has a composition series.

$\{e\} = H_0 \Delta H_1 \Delta \cdots \Delta H_n = G$ where $H_i \Delta H_{i+1}$

& $\frac{H_{i+1}}{H_i}$ is simple.

Now, G is solvable $\Rightarrow$ H_i is solvable $\forall i$.

$\Rightarrow \frac{H_{i+1}}{H_i}$ is solvable

[Quotient grp. of solvable grp is solvable]

$\Rightarrow \frac{H_{i+1}}{H_i}$ is simple & solvable.

$\Rightarrow \frac{H_{i+1}}{H_i}$ is Abelian.

$\therefore$ All subgroups of $\frac{H_{i+1}}{H_i}$ are normal.

Since. $\frac{H_{i+1}}{H_i}$ is simple.

It has no non-trivial proper subgrps.

i.e $\frac{H_{i+1}}{H_i}$ has only 2 normal subgrps.

$\Rightarrow \left|\frac{H_{i+1}}{H_i}\right|$ is prime.

$\Rightarrow$ As every grp. of Prime order is cyclic.

$\Rightarrow \frac{H_{i+1}}{H_i}$ is a cyclic grp.

$\Leftarrow$ Converse As $\frac{H_{i+1}}{H_i}$ is cyclic.

$\Rightarrow \frac{H_{i+1}}{H_i}$ is abelian.

$\Rightarrow G$ is solvable.

(iii) All composition factors of G are of prime order

As proved (earlier)

Above $\frac{H_{i+1}}{H_i}$ is of prime order.

(iv) As G has a Composition Series.

$\Rightarrow 1 = H_0 \Delta H_1 \Delta H_2 \cdots \Delta H_n = G$ s.t $H_i \Delta H_{i+1}$

Page No. 164

& $\frac{H_{i+1}}{H_i}$ is cyclic.

As every cyclic grp is abelian.

$\Rightarrow \frac{H_{i+1}}{H_i}$ is abelian.

(Ch-6, prop-10 I)

Theorem let $H \Delta G$. If both H & $\frac{G}{H}$ are solvable then G is solvable.

Pf:— let $\frac{G}{H} = \frac{G_0}{H} \supseteq \frac{G_1}{H} \supseteq \frac{G_2}{H} \supseteq \cdots \supseteq \frac{G_{m-1}}{H} \supseteq \frac{G_m}{H} = \{e\}$ —(1)

be a solvable series for G/H.

Here each G_i is subgrp. of G containing H.

Since $\frac{G_{i+1}}{H} \Delta \frac{G_i}{H}$

$\Rightarrow G_{i+1} \Delta G_i$

Also, $\frac{G_m}{H} = \{e\} \Rightarrow G_m = H$

Now, let $\{e\} = H_n \subseteq H_{n-1} \subseteq H_{n-2} \subseteq \cdots \subseteq H_1 \subseteq H_0 = H$ —(2)

be a solvable series for H.

Then $\{e\} = H_n \subseteq H_{n-1} \subseteq \cdots \subseteq H_1 \subseteq H_0 = H = G_m \subseteq G_{m-1}$

$\subseteq G_{m-2} \subseteq \cdots \subseteq G_0 = G$ is a solvable series for G.

$\Rightarrow G$ is solvable.

(Ch-6, prop-10, II)

Theorem P.T Homomorphic image of a solvable grp is solvable.

Pf:— let G be solvable grp.

let H be a homomorphic image of G. i.e

$\exists$ a homomorphism $\phi: G \to H$ that is onto.

$\phi: G \to H$ is a H.M & onto

As G is solvable $\Rightarrow \exists$ a +ve integer K s.t $G^{(k)} = \{e\}$

T.P

H is solvable, we have to Prove $H^{(k)} = \{e'\}$

where e' is identity of H.

Now, $x^{-1}y^{-1}xy \in G$. Then $x^{-1}y^{-1}xy$ is a commutator.

$\Rightarrow x^{-1}y^{-1}xy \in G'$.

Then.

$$\phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y)$$
$$= (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y)$$

is again a commutator.

$\Rightarrow \phi(x^{-1}y^{-1}xy) \in H'$

$\Rightarrow \phi(G') = H'$ $[\because \phi$ is onto$]$

||'rly $H^{(2)} = (H')' = (\phi(G'))' = \phi(G^{(2)})$

||'rly $H^{(k)} = \phi(G^{(k)}) = \phi(\{e\}) = \{e'\}$

$\Rightarrow H^{(k)} = \{e'\}$

$\Rightarrow H$ is solvable.

* * *

Q	1	2	4	5	7	8	9
P	160	156		160		162	

All study Materials Related to CSIR-NET, GATE, JAM, CUCET, SET/SLET, PSC, ..etc are available at www.pkalika.wordpress.com

= P. Kalika

Page No. 84

External Direct Product

Let $G_1, G_2, \ldots G_n$ be finite collection of groups. Then

$G_1 \oplus G_2 \oplus \ldots \oplus G_n$ = set of the n-tuples of the the form $\{(g_1, g_2, \ldots g_n) \mid g_i \in G_i\}$

$G_1 \oplus G_2 \oplus \ldots \oplus G_n$ is a group under componentwise [addition or multiplication] operation

$(g_1, g_2, \ldots g_n)(g_1', g_2', g_3', \ldots g_n') = (g_1 g_1', g_2 g_2', \ldots g_n g_n')$

(i) Closure prop:

$(g_1, g_2, \ldots g_n)(g_1', g_2', \ldots g_n') = (g_1 g_1', g_2 g_2', \ldots g_n g_n')$
$\in G_1 \oplus G_2 \oplus \ldots \oplus G_n$
$\forall\ g_i, g_i' \in G_i$

(ii) Associativity:

$(g_1, g_2, \ldots g_n)(g_1', g_2', \ldots g_n')(g_1'', g_2'', \ldots g_n'')$
$= (g_1 g_1', g_2 g_2', \ldots g_n g_n')(g_1'', g_2'', \ldots g_n'')$
$= ((g_1 g_1') g_1'', (g_2 g_2') g_2'', \ldots (g_n g_n') g_n'')$
$= (g_1 (g_1' g_1''), g_2 (g_2' g_2''), \ldots g_n (g_n' g_n''))$
$= (g_1, g_2, \ldots g_n)((g_1', g_2', \ldots g_n')(g_1'', g_2'', \ldots g_n''))$

(iii) $(e_1, e_2, \ldots e_n) \in G_1 \oplus G_2 \oplus \ldots \oplus G_n$
where $e_i \in G_i$ be identity of G_i

(iv) Inverse: $(g_1, g_2, \ldots g_n) \in G_1 \oplus G_2 \oplus \ldots \oplus G_n$.
Then $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \in G_1 \oplus G_2 \oplus \ldots \oplus G_n$
is inverse of $(g_1, g_2, \ldots g_n)$.

Page No. 85

Date

Note:- $O(G_1 \oplus G_2 \oplus \cdots \oplus G_n) = O(G_1) \oplus (G_2) \cdots O(G_n)$

Eg-1 Consider $U(8) \oplus U(10)$

$U(8) = \{1, 3, 5, 7\}$ $\odot_8$

$U(10) = \{1, 3, 7, 9\}$ $\odot_{10}$

$U(8) \oplus U(10) = \{(1,1), (1,3), (1,7), (1,9), (3,1)$
$(3,3), (3,7), (3,9), (5,1), (5,3), (5,7), (5,9)$
$(7,1), (7,3), (7,7), (7,9)\}$

$(3,7) \cdot (7,9) = (5,3)$
mod 8, mod 10.

$U(8) \oplus U(10)$ is a group under component-wise operation. $(1,1)$ is identity of $U(8) \oplus U(10)$

order of $(1,7)$ $O[U(8) \oplus U(10)] = 16$

Order of each element is a factor of 16
i.e $1, 2, 4, 8, 16$.

$(1,7)^2 = (1,7)(1,7) = (1,49) = (1,9) = 2$

$(1,7)^3 = (1,7)(1,9) = (1,63) = (1,3) = 4$

$(1,7)^4 = (1,7)(1,3) = (1,21) = (1,1) = 2$

$\Rightarrow$ Order of $(1,7) = 4$

inverse of $(1,7)$ is $(1,3)$.

Find inverse of $(5,7) = ?$

$(5,7)(5,3) = (25, 21) = (1,1)$

$\Rightarrow$ inverse of $(5,7) = (5,3)$

Ex-2 $Z_2 \oplus Z_3$, $Z_2 = \{0, 1\}$, $Z_3 = \{0, 1, 2\}$

$Z_2 \oplus Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Page No. 86
Date

$Z_2 \oplus Z_3$ is an abelian group of order '6'.

Operation is componentwise addition.
$Z_2 \oplus Z_3$ is a cyclic group generated by $(1,1)$

$1(1,1) = (1,1)$
$2(1,1) = (2,2) = (0,2)$
$3(1,1) = (3,3) = (1,0)$
$4(1,1) = (4,4) = (0,1)$
$5(1,1) = (5,5) = (1,2)$
$6(1,1) = (6,6) = (0,0)$

$\Rightarrow$ $(1,1)$ is of order '6' $\Rightarrow$ $(1,1)$ is generator of $Z_2 \oplus Z_3$
As we know that a finite cyclic group of order '6' is isomorphic to Z_6.
$\Rightarrow Z_2 \oplus Z_3 \simeq Z_6$

Consider $Z_2 \oplus Z_2$
To Prove $Z_2 \oplus Z_2 \not\simeq Z_4$.

$Z_2 \oplus Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$
order of $(0,1) = 2$
Order of $(1,0) = 2$
$(1,1) = 2$
There is no element of order 4
$\Rightarrow Z_2 \oplus Z_2$ is not cyclic
Hence $Z_2 \oplus Z_2 \not\simeq Z_4$.

Properties of External Direct product:

Theorem (8.1) The order of an element of a Direct product of a finite no. of group is the least

Page No. 87
Date

Common multiple of the orders of the components of the element i.e

$$|(g_1, g_2, \ldots g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots |g_n|)$$

Pf: let us consider the special case for $n=2$.

i.e T.S $O(g_1, g_2) = \text{lcm}[O(g_1), O(g_2)]$

Let $s = \text{lcm of } [O(g_1), O(g_2)]$

Let $t = O(g_1, g_2) \rightarrow O(g_1) | s \Rightarrow g_1^s = e_1$

$(g_1, g_2)^s = (g_1^s, g_2^s)$ $\quad O(g_2) | s \Rightarrow g_2^s = e_2$

$= (e_1, e_2)$

If $(g_1, g_2)^s = (e_1, e_2)$, then

$(g_1^s, g_2^s) = (e_1, e_2) \Rightarrow$ But $O(g_1, g_2) = t$

$\Rightarrow t | s$

Also, $(g_1^t, g_2^t) = (g_1, g_2)^t = (e_1, e_2)$

$\Rightarrow O(g_1) | t, \; O(g_2) | t$

$\Rightarrow t$ is a common factor of $O(g_1)$ & $O(g_2)$

$\Rightarrow s | t \Rightarrow s = t$

Eg-3 Determine the no. of elements of order 5 in $Z_{25} \oplus Z_5$.

Soln. If $(a, b) \in Z_{25} \oplus Z_5$ has order 5, then

$O[(a,b)] = 5 = \text{lcm}[O(a), O(b)]$

Clearly, either $O(a) = 5$ and $O(b) = 1$ or 5

or $O(b) = 5$ and $O(a) = 1$ or 5

Page No. 28
Date

Case-I $o(a) = 1$, $o(b) = 5$
$\Rightarrow$ there is only one choice for a i.e $a = 0$ and 4 choices for $b = 1, 2, 3, 4$.
$\Rightarrow$ There are four elts of order 5.
$\Rightarrow (0,1), (0,2), (0,3), (0,4)$.

Case-2 $o(a) = 5$ & $o(b) = 1$
There is only one choice for $b = 0$ & 4 choices for 'a' i.e, 5, 10, 15, 20.
$\boxed{(5,0), (10,0), (15,0), (20,0)}$

Case-3. $o(a) = 5$ & $o(b) = 5$.
four choices for $a = 5, 10, 15, 20$ & four Choices for $b = 1, 2, 3, 4$.
There are 16 elts of order '5'.
$\Rightarrow Z_{25} \oplus Z_5$ has 24 elts of order 5.

Ex. 4 Determine the no. of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$.

Soln:- Let us first find elts. in $Z_{100} \oplus Z_{25}$ of order 10.
If $(a,b) \in Z_{100} \oplus Z_{25}$ has order 10, then $o[(a,b)] = 10 = \text{lcm}[o(a), o(b)]$
So, 2 cases arises —
(i) $o(a) = 10$, $o(b) = 1$ or 5.
(ii) $o(a) = 2$, $o(b) = 5$

$o(b)$ Can't be 10
$o(b)$ Can't be 2

Case-I $o(a) = 10$ & $o(b) = 1$ or 5.
Since Z_{100} has a unique cyclic subgp. of order 10 & only cyclic group of order 10 has four generators.

Page No. 89
Date

[$\because$ $G = \langle a \rangle$ of order n. then $G = \langle a^k \rangle$ for $(k, n) = 1$]

Here $n = 10$.
$k = 1, 3, 7, 9$]

If H is a cyclic subgroup of 10 then $H = \langle a \rangle$ or $\langle a^3 \rangle$ or $\langle a^7 \rangle$ or $\langle a^9 \rangle$
$\Rightarrow$ There are four choices of 'a'
llly, there are 5 choices for 'b'.
$\Rightarrow$ Total choices for $(a, b) = 20$,

Case-II $\boxed{O(a) = 2;\ O(b) = 5}$

Since Z_{100} has a unique cyclic subgroup of order 'n' & that subgroup has only one generator.
$\because$ If k is a cyclic group of order 2 then $k = \langle a \rangle$, $O(a) = 2$.
$\Rightarrow$ There is only one choice for 'a' there are 4 choices for 'b'.
$\Rightarrow$ There are four choices for (a, b)
$\Rightarrow$ $Z_{100} \oplus Z_{25}$ has 24 elts of order 10.

let k be a cyclic subgroup of $Z_{100} \oplus Z_{25}$ of order 10.

$\boxed{\text{order of the subgp } k = 10}$ $k = \langle (x, y) \rangle$

No. of generators of $k = 4$
$= \phi(10)$ $O(x, y) = 10$

i.e 4 elts of order 10 generate the same subgroup.
$\therefore$ No. of cyclic subgp of order 10
$= \frac{24}{4} = 6$

Ex-4 Find the no. of elts in $\langle 5\rangle \oplus \langle 3\rangle$ as a subgp. of $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$.

Sol^n: Since order of 5 in $\mathbb{Z}_{30}$ is '6'.
order of 3 in $\mathbb{Z}_{12}$ is '4'.
$\Rightarrow$ $\langle 5\rangle \oplus \langle 3\rangle$ has a subgrp of order 24.
$\because O(\langle 5\rangle \oplus \langle 3\rangle) = O(\langle 5\rangle)\, O(\langle 3\rangle)$
$= 6 \cdot 4 = 24$

Thm (8.2) CRITERION FOR $G \oplus H$ TO BE CYCLIC

(M 2019)

Let G & H be finite cyclic groups. Then $G \oplus H$ is cyclic if & only if $|G|$ & $|H|$ are relatively prime.

Pf:- Let $|G| = m$ & $|H| = n$
$\Rightarrow |G \oplus H| = |G| \cdot |H| = mn$

First Part

let $G \oplus H$ be cyclic.
T.S $\gcd(m,n) = 1$
let $\gcd(m,n) = t$, s.t $t \neq 1$.
Since G is cyclic $\Rightarrow \exists$ $g \in G$ s.t $G = \langle g\rangle$
$\Rightarrow |g| = m$
H is cyclic $\Rightarrow \exists$ $h \in H$ s.t $H = \langle h\rangle$
$\Rightarrow |H| = n$.
As $t|m$ & $t|n$ $\Rightarrow m = \lambda t$, $n = ut$
$\Rightarrow \lambda = \frac{m}{t}$, $u = \frac{n}{t}$

If $(g^{\frac{m}{t}})^k = g^{\lambda k} = e$
$\Rightarrow m \mid \lambda k \Rightarrow \lambda t \mid \lambda k$
$\Rightarrow t \mid k$

Consider $O(g^{m/t}) = ?$

$\left(g^{\frac{m}{t}}\right)^t = g^{m t/t} = g^m = e$

$\Rightarrow O\left(g^{m/t}\right) = t$ & $O\left(h^{n/t}\right) = t$.

Consider $\left(g^{m/t}, e_2\right), \left(e_1, h^{n/t}\right) \in G \oplus H$

$$O\left(g^{m/t}, e_2\right) = t = O\left(e_1, h^{n/t}\right)$$

$\Rightarrow \langle\left(g^{m/t}, e_2\right)\rangle$ & $\left(e, h^{n/t}\right)$ are two distincts cyclic subgrps of $G \oplus H$ of order 't'. which is a contradiction.

[$\because$ Any finite cyclic grp. has a unique subgrp of order t].

$\Rightarrow \gcd(m, n) = 1$.

$\Leftarrow$ let $G = \langle g\rangle$ & $(m, n) = 1$, $H = \langle h\rangle$

then

$$|(g\, h)| = \text{lcm}\left[\,|g|, |h|\,\right]$$
$$= \text{lcm}(m, n) = mn$$
$$= |G \oplus H|$$

$\Rightarrow G \oplus H = \langle (g, h)\rangle$

$\Rightarrow G \oplus H$ is a cyclic group.

Corollary: An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite no. of finite cyclic group is cyclic iff $|G_i|$ & $|G_j|$ are relatively prime for $i \neq j$.

Cor. $\boxed{\text{Criterion for } Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}}$

let $m = n_1 n_2 \cdots n_k$ then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ iff n_i & n_j are relatively prime where $i \neq j$.

Page No. 92
Date

Sol^n $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ is cyclic iff n_i & n_j are relatively prime.

$\because \quad |Z_{n_i}| = n_i$

$|Z_{n_j}| = n_j$

& also any 2 finite cyclic grps of same order are isomorphic therefore —

$Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$

(i) $Z_2 \oplus Z_3 \approx Z_6$

(ii) $Z_2 \oplus Z_3 \oplus Z_5 \approx Z_{30} \approx Z_2 \oplus Z_{15} \approx Z_6 \oplus Z_5$

(iii) $Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5$

$\approx Z_6 \oplus Z_{10}$

$\approx Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5$

(iv) But $Z_2 \oplus Z_{30} \not\approx Z_{60}$

U(n) as an EDP

Theorem 8.3 (154) Let $\gcd(s,t) = 1$, then

$U(st) \approx U(s) \oplus U(t)$

No. of elts in $U(n) = \phi(n)$

$\phi(n)$ = No. of +ve integers less than n & co-prime to n.

Eg. $|U(8)| = \phi(8)$. $\Big\{ \because 1, 3, 5, 7$ are integers less than 8 and relatively co-prime to 8

$\phi(8) = 4$

So $|U(st)| = \phi(st)$

$|U(s) \oplus U(t)| = |U(s)|\,|U(t)|$

$= \phi(s) \cdot \phi(t)$

Since $\gcd(s,t) = 1$

$\Rightarrow \phi(st) = \phi(s)\phi(t)$

$\Rightarrow |U(st)| = |U(s) \oplus U(t)|$

Page No. 93

$\therefore$ we can define a map betn $U(st)$ & $U(s) \oplus U(t)$ which is 1-1 will be onto.

Define $f: U(st) \to U(s) \oplus U(t)$ as
$$f(x) = (x \bmod s,\ x \bmod t)$$

well defined   let $x = y$
$$\Rightarrow x \bmod s = y \bmod s$$
$$\& \quad x \bmod t = y \bmod t$$
$$\Rightarrow (x \bmod s,\ x \bmod t) = (y \bmod s,\ y \bmod t)$$
$$\Rightarrow f(x) = f(y).$$

1-1   let $f(x) = f(y)$
$$\Rightarrow (x \bmod s,\ x \bmod t) = (y \bmod s,\ y \bmod t)$$
$$\Rightarrow x \bmod s = y \bmod s$$
$$\& \quad x \bmod t = y \bmod t$$
$\because \gcd(s,t) = 1 \Rightarrow x \bmod st = y \bmod st$
$$\Rightarrow st \mid x-y$$
$$\Rightarrow x - y = kst \quad \text{for some } k \in \mathbb{Z}$$
$$st \mid x-y \Rightarrow x - y = 0$$
$$\Rightarrow x = y. \quad f \text{ is } 1\text{-}1.$$

H.M $f(xy) = (xy \bmod s,\ xy \bmod t)$

$f(x) f(y) = (x \bmod s,\ x \bmod t)(y \bmod s,\ y \bmod t)$
$= ((x \bmod s)(y \bmod s) \bmod s,\ (x \bmod t)(y \bmod t) \bmod t)$
$= (xy \bmod s,\ xy \bmod t)$

[$\because$ $(a \bmod n)(b \bmod n) \bmod n = ab \bmod n$]

$\Rightarrow f$ is an Isomorphic

$\Rightarrow U(st) \approx U(s) \oplus U(t).$

Eg: $U(105) \approx U(7) \oplus U(15)$ $(7,15)=1$
$U(105) \approx U(21) \oplus U(5)$ $(21,5)=1$
$U(105) \approx U(3) \oplus U(7) \oplus U(5)$

* Consider $U_k(n) = \{x \in U(n) ; x \equiv 1 \bmod k\}$
where k is a divisor of 'n'.
$U_k(n)$ is a subgrp of $U(n)$.

Theorem 8.3 (p-154) Let $\gcd(s,t)=1$, Then
$U_s(st) \approx U(t)$ & $U_t(st) \approx U(s)$

Pf: Define $f: U_s(st) \to U(t)$
$f(x) = x \bmod t$
$g: U_t(st) \to U(s)$ as $g(x) = x \bmod s$.
PT f & g are isomorphic

Corollary Let $m = n_1 n_2 \ldots n_k$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$.
Then
$U(m) \approx U(n_1) \oplus U(n_2) \oplus U(n_3) \oplus \ldots \oplus U(n_k)$

Note: (i) $U(2) \approx \{0\}$
(ii) $U(4) \approx Z_2$
(iii) $U(2^n) \approx Z_2 \oplus Z_{2^{n-2}}$ $\forall n \geq 3$
(iv) $U(p^n) \approx Z_{p^n - p^{n-1}}$ for odd prime p.

Eg Show $U(105) \approx Z_2 \oplus Z_4 \oplus Z_6$.
$U(105) = U(3 \cdot 7 \cdot 5)$
$\approx U(3) \oplus U(5) \oplus U(7)$
$\approx Z_2 \oplus Z_4 \oplus Z_6$ (By Above)

$U(720) = U(5 \cdot 9 \cdot 16)$
$\approx U(5) \oplus U(3^2) \oplus U(2^4)$
$\approx \cancel{Z_{20}}\ Z_4 \oplus Z_6 \oplus Z_2 \oplus Z_4$
$\approx \cancel{Z_2 \oplus}$

(vii) PT There are 96 Automorphism of Z_{720} of order 12.

pf: Since $U(n) \approx Aut(Z_n)$

$\therefore U(720) \approx Aut(Z_{720})$

$\therefore$ It is sufficient to show that there are 96 elts of $U(720)$ of order 12.

Now $U(720) \approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$

It is sufficient to find elts of order 12 in $Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$

Let $(a,b,c,d) \in Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$ be of order 12.

i.e $|(a,b,c,d)| = 12$.

Now, $|(a,b,c,d)| = lcm(|a|, |b|, |c|, |d|)$

Since, $a \in Z_2$ $\therefore a = 0$, or $a = 1$

$\therefore |a| = 1$ or 2

$\Rightarrow lcm(|a|,|b|,|c|,|d|) = lcm(|b|,|c|,|d|)$

Case I $\boxed{o(b) = 4, o(c) = 3 \text{ or } 6, o(d) = 2 \text{ or } 4}$

Arbitrary

There are 2 choices for b

4 ——— c

4 ——— d

$\therefore$ Total choices $= 2 \cdot 4 \cdot 4 = 32$

Case-II. $\boxed{o(b) = 1 \text{ or } 2, o(c) = 3 \text{ or } 6, o(d) = 4}$

There are 2 choices for b.

4 ——— c

2 ——— d

$\Rightarrow$ Total choices $= 2 \cdot 4 \cdot 2 = 16$

Hence $\text{lcm}(|b|, |c|, |d|) = 12$ in $32+16 = 48$ ways

Since $o(a) = 1$ or 2.

$\text{lcm}(|b|, |c|, |d|) = 12$ in $48 \times 2 = 96$ ways

$\Rightarrow$ There are 96 ~~ways~~ Automorphism of Z_{120} of order 12.

Chapter- End

* * *

CHAPTER- 9

(only, Internal Direct Product) (P-181)

Let H & K be normal subgps of a grp. G. Then G is the Internal direct Product of H & K & $G = H \times K$ if

(i) $G = HK$ &

(ii) $H \cap K = \{e\}$

Note:- For Internal direct product :- H & K must be subgps of the same group.

For External Direct product :- H & K can be any groups.

Ex:- Let $G = S_3$

$= \{I, (12), (23), (13), (123), (132)\}$

Let $H = \langle (123) \rangle = \{I, (123), (132)\}$

$K = \langle (12) \rangle = \{I, (12)\}$

G is internal direct product of H & K where $G \simeq H \oplus K$

Now $HK = \langle (123) \rangle \langle (12) \rangle$

$= \{I, (12), (123), (123)(12), (132), (132)(12)\}$

Page No. 97
Date

$HK = \{I, (12), (13), (23), (123), (132)\}$

Now Here $G = HK$ & $H \cap K = \{e\}$

But $G \not\cong H \oplus K$

$\because H \oplus K$ is cyclic & S_3 is not

$H \oplus K = \{(I, I), ((123), (12)), ((123), I), (I, (12)), ((132), I), ((132), (12))\}$

$|H \oplus K| = 6$

$|((132), (12))| = 6$

$H \oplus K$ is cyclic. But S_3 is not

$\because$ there is no elt. of order 6 in S_3

$\Rightarrow G$ is not an IDP.

(as K is not normal)

Defn: **Internal Direct Product of $H_1 \times H_2 \times \dots \times H_n$** :—

let $H_1, H_2, \dots, H_n$ be finite collection of normal subgrp of G. Then G is the IDP of $H_1 \times H_2 \times \dots \times H_n$ if

(i) $G = H_1 H_2 \cdots H_n$

(ii) $(H_1 \cdot H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ $\forall i = 1, 2, 3 \dots n-1$.

or if G is an IDP of $H_1, H_2, \dots H_n$ then $H_i \cap H_j = \{e\}$ $\forall i \neq j$

Lemma 1:— let G be the IDP of H & K, then elements of H & K commute i.e $hk = kh$ $\forall h \in H, k \in K$

Pf: G is IDP of H & K

$\Rightarrow H \triangle G$ & $K \triangle G$ & $G = HK$ & $H \cap K = \{e\}$

TP: $hk = kh$ $\forall h \in H$ & $k \in K$.

Consider, $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in hH = H$

Page No. 98
Date

$\because kh^{-1}k^{-1} \in kHk^{-1} \quad \forall k \in K \Rightarrow k \in G$
and as $H \triangle G$
$\Rightarrow kHk^{-1} \subseteq H \Rightarrow kh^{-1}k^{-1} \in H$

IIrly., $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in Kk^{-1}$
$= K \; (K \triangle G)$
$\Rightarrow hkh^{-1}k^{-1} \in H \cap K = \{e\}$
$\Rightarrow hkh^{-1}k^{-1} = e$
$\Rightarrow hk = kh \quad \forall h \in H, \; k \in H$

Result: $\boxed{\text{So, if } G \text{ is IDP of } H_1, H_2, \ldots H_n, \text{ then } h_i h_j = h_j h_i \;\; \forall h_i \in H_i, h_j \in H_j, \; i \neq j}$

Lemma-2. If G is the IDP of $H_1, H_2, \ldots H_n$. then each member of G can be expressed uniquely as $h_1, h_2, \ldots, h_n$ where $h_i \in H_i$.

Pf: G is IDP of $H_1, H_2, \ldots H_n$
$\Rightarrow G = H_1 \times H_2 \times \cdots \times H_n$. iff ——

(i) $G = H_1 H_2 \cdots H_n$. & $H_i \cap H_j = \{e\}$, $i \neq j$
or $[(H_1; H_2, \ldots H_i) \cap H_{i+1}] = \{e\}$, $i = 1, 2, 3 \ldots n-1$.
Let
$x \in G$
$\therefore x \in H_1 H_2 \cdots H_n$
$\Rightarrow x = h_1 h_2 \cdots h_n$ for some $h_i \in H_i$

Uniqueness:
Let $x = h_1 h_2 \cdots h_n$, $h_i, h_i' \in H_i$
& $x = h_1' h_2' \cdots h_n'$
$\Rightarrow h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$
$(h_1 h_2 \cdots h_{n-1}) h_n (h_n')^{-1} = (h_1' h_2' \cdots h_{n-1}')$
$\Rightarrow h_n (h_n')^{-1} = (h_1 h_2 \cdots h_{n-1})^{-1} (h_1' h_2' \cdots h_{n-1}')$

$= (h_1^{-1}h_1')(h_2^{-1}h_2') \cdots (h_{n-1}^{-1}h_{n-1}')$

$\Rightarrow h_n(h_n')^{-1} \in H_1H_2 \cdots H_{n-1}$

$\Rightarrow h_n(h_n')^{-1} \in H_n \cap (H_1H_2 \cdots H_{n-1}) = \{e\}$

$\Rightarrow h_n(h_n')^{-1} = e$

$\Rightarrow h_n = h_n'$

$\Rightarrow h_1h_2 \cdots h_{n-1} = h_1'h_2' \cdots h_{n-1}'$

IIly $h_1 = h_1', \ h_2 = h_2', \ \cdots \ h_n = h_n'$

Theorem (9.6) 2014 $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$. If a Group G is the IDP of a finite no. of subgrps $H_1, H_2, \ldots, H_n$ then G is isomorphic to the external Direct product of $H_1, H_2, \ldots H_n$.

Pf:— $G \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$ —— (1)

As G is the IDP of $H_1, H_2, \ldots, H_n$

$\Rightarrow H_i \trianglelefteq G \ \forall i$

& $G = H_1H_2 \cdots H_n$ & $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$

$i = 1, 2, 3 \ldots n-1$

T.P Define a map $\phi: G \to H_1 \oplus H_2 \oplus \cdots \oplus H_n$

as $\phi(h_1h_2 \cdots h_n) = (h_1, h_2, \cdots h_n)$

T.P ϕ is well define, 1-1, HM & onto.

well-Define & 1-1

let $h_1h_2 \cdots h_n = h_1'h_2' \cdots h_n'$

$\Leftrightarrow h_i = h_i' \ \forall i$ (By lemma)

$\Leftrightarrow (h_1, h_2, \cdots h_n) = (h_1', h_2', h_3', \cdots h_n')$

$\Leftrightarrow \phi(h_1h_2 \cdots h_n) = \phi(h_1'h_2' \cdots h_n')$

H.M $\phi((h_1h_2 \cdots h_n)(h_1'h_2' \cdots h_n'))$

$= \phi(h_1h_1'h_2h_2' \cdots h_nh_n')$ [By I lemma]

Page No. 106
Date

$= (h_1h_1', h_2h_2', \dots h_nh_n')$
$= (h_1, h_2, \dots h_n)(h_1', h_2', \dots h_n')$
$= \phi(h_1, h_2, \dots h_n)\ \phi(h_1' h_2' \dots h_n')$

<u>Onto</u> let $(y_1, y_2, \dots y_n) \in H_1 \oplus H_2 \oplus \dots \oplus H_n$
$\Rightarrow y_i \in H_i$
$\Rightarrow \exists\ y_1, y_2, \dots y_n \in H_1, H_2, \dots H_n$
S.t. $\phi(y_1 y_2 \dots y_n) = (y_1, y_2, \dots y_n)$
$\Rightarrow G \approx H_1 \oplus H_2 \oplus \dots \oplus H_n$

<u>Result:</u> If $G = H_1 \oplus H_2 \oplus \dots \oplus H_n$ then G can be expressed as the IDP of subgroups isomorphic to $H_1, H_2, \dots H_n$.

eg. If $G = H_1 \oplus H_2$
then $G = \overline{H_1} \times \overline{H_2}$ where $\overline{H_1} = H_1 \oplus \{e\}$
$\overline{H_2} = \{e\} \oplus H_2$
$H_1 \approx \overline{H_1}$ & $H_2 \approx \overline{H_2}$

Eg. Express $U(105)$ as IDP of 2 subgroups.

$U(105) = U(15 \cdot 7) \approx U(15) \oplus U(7)$
[$\because U(st) \approx U(s) \oplus U(t)$, if $(s,t) = 1$]
Also, $U_s(st) \approx U(t)$
So $U_7(105) \approx U(15)$
& $U_{15}(105) \approx U(7)$

$\Rightarrow U(105) \approx U_7(105) \oplus U_{15}(105)$
$\approx U_7(105) \times U_{15}(105)$
$\because H_1 \oplus H_2 \approx H_1 \times H_2$ if H_1 & H_2 are subgrp. of G if $k|n \Rightarrow U_k(n) < U(n)$
Also, $U(105) = U(5 \cdot 21) = U_5(105) \times U_{21}(105)$
$\approx U(21) \oplus U(5)$.

Page No. 102

$\cong U(21) \oplus U(5)$.

Eg. Express $U(105)$ as IDP of 3 subgps.

$$U(105) = U(3.5.7)$$
$$= U_{35}(105) \times U_{21}(105) \times U_{15}(105)$$
$$= \{1, 71\} \times \{1, 22, 43, 64\} \times \{1, 16, 31, 46, 61, 76\}$$
$$\approx U(3) \oplus U(5) \oplus U(7)$$

(1) Show that $G \oplus H$ is abelian iff G & H are abelian.

Sol^n: let $G \oplus H$ be abelian.
Let (g_1, h_1) & $(g_2, h_2) \in G \oplus H$ where $g_1, g_2 \in G$, $h_1, h_2 \in H$

Now, $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$
$\Rightarrow (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1)$
$\Rightarrow g_1 g_2 = g_2 g_1$
$h_1 h_2 = h_2 h_1$ $\quad \therefore G$ & H are Abelian.

($\Leftarrow$) Let G & H be Abelian.
Consider $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ $\quad \forall (g_1, h_1), (g_2, h_2) \in G \oplus H$
$= (g_2 g_1, h_2 h_1)$
$= (g_2, h_2)(g_1, h_1)$

(5) Prove or Disprove that $Z \oplus Z$ is a cyclic group.

Pf: Let if possible $Z \oplus Z$ is cyclic.
$\Rightarrow \exists (a, b) \in Z \oplus Z$ s.t $Z \oplus Z = \langle (a, b) \rangle$
(i) if $a = b$.

Page No. 102
Date

$\mathbb{Z} \oplus \mathbb{Z} = \langle (a,a) \rangle$

Then $(m,n) \in \mathbb{Z} \oplus \mathbb{Z}$ can't be written as integral multiple of (a,a) in ~~many~~ any way.

(ii) If $a \neq b$.
Then all elts of the form (m,m) don't belong to $\mathbb{Z} \oplus \mathbb{Z}$, $\therefore$ (m,m) can't be written as integral multiple of (a,b).
$\Rightarrow$ $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

Q. 6 Show that $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

$|\mathbb{Z}_8 \oplus \mathbb{Z}_2| = 16 = |\mathbb{Z}_4 \oplus \mathbb{Z}_4|$

Pf:- order of elts of $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ are $1, 2, 4, 8$
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$ are $1, 2, 4$
There is no elt. of order 8 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$
$\therefore$ $\mathbb{Z}_8 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$

Q(17) What is the order of any non-identity elt. of $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$??

Pf:- let (a,b,c) be any non-id elt. of $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
$O(a,b,c) = \text{lcm}\,[|a|, |b|, |c|]$
But $a, b, c \in \mathbb{Z}_3$, the only possible order are 1 & 3.
as $(a,b,c) \neq (0,0,0)$
$\therefore$ at least one of $|a|, |b|, |c|$ is 3.
$\Rightarrow$ $O(a,b,c) = \text{lcm}\,[|a|, |b|, |c|] = 3$.

2014

(18) How many subgroup of order 4 does $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ have?

Sol: $\mathbb{Z}_4 \oplus \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)\}$
$\langle (a,b) \rangle$ is a subgroup of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ if $|(a,b)| = 4$

Page No. 103
Date

elts of order 4 in $Z_4 \oplus Z_2$ are
$(1,1), (1,0), (3,0), (3,1)$

[Result :-
$|G|=n$ $G = \langle a \rangle$, then $G = \langle a^k \rangle$ iff $(k,n)=1$]

Let H be a ~~group~~ subgp. of $Z_4 \oplus Z_2$ of order 4.

$$H = \langle (1,1) \rangle$$

then, $H = \langle (1,1)^3 \rangle = \langle (3,3) \rangle = \langle (3,1) \rangle$

$\therefore$ subgps of order 4 generated by $(1,1)$ & $(3,1)$ are same —

$$\langle (1,1) \rangle = \langle (3,1) \rangle$$

Now, the subgp. $K = \langle (1,0) \rangle$, $|K| = 4$

$$= \langle (1,0)^3 \rangle$$
$$= \langle (3,0) \rangle$$

$\Rightarrow$ No. of distinct cyclic gps of order 4 are,

$$H = \langle (1,1) \rangle$$
$$K = \langle (1,0) \rangle$$

Also, $L = \{(0,0), (0,1), (2,0), (2,1)\}$ is a non-cyclic gp of order 4.

$\therefore Z_4 \oplus Z_2$ has 3 subgp. of order 4.

(23) Find all subgps of order 3 in $Z_9 \oplus Z_3$.

(2013) Groups of prime order are cyclic

Now, subgroup of order 3 must be cyclic.
So, we have to find cyclic gps. of order 3 in $Z_9 \oplus Z_3$.

Let $(a,b) \in Z_9 \oplus Z_3$ s.t. $|(a,b)| = 3$

$|(a,b)| = \text{lcm}\,[|a|, |b|]$

$\lvert a\rvert = 1$ or 3	$\lvert a\rvert = 1$.	$\lvert b\rvert = 3$
$\lvert b\rvert = 1$ or 3	$\lvert a\rvert = 3$	$\lvert b\rvert = 1$
	$\lvert a\rvert = 3$	$\lvert b\rvert = 3$

elts. of order 3 in $Z_9 \oplus Z_3$ are
$(0,1), (0,2), (3,0), (3,1), (3,2), (6,0), (6,1), (6,2)$.

Now $H_1 = \langle(0,1)\rangle = \langle(0,1)^2\rangle = \langle(0,2)\rangle$

[$G = \langle a\rangle = \langle a^k\rangle$ iff $(k,n) = 1$]
$|a| = n$

$H_2 = \langle(3,0)\rangle = \langle(3,0)^2\rangle = \langle(6,0)\rangle$

$H_3 = \langle(3,1)\rangle = \langle(3,1)^2\rangle = \langle(6,2)\rangle$

$H_4 = \langle(3,2)\rangle = \langle(3,2)^2\rangle = \langle(6,4)\rangle$
$= \langle(6,1)\rangle$

∴ No. of distinct subgroups of order 3 are $\langle(0,1)\rangle, \langle(3,0)\rangle, \langle(3,1)\rangle, \langle(3,2)\rangle$

Q. 35) Prove that $D_3 \oplus D_4 \not\cong D_{24}$

Pf:- Every Rotation in D_{24} has order 24.
Now, we'll prove that $D_3 \oplus D_4$ has no elt. of order 24.
Any Rotation in D_3 has order 3 & ~~reflection about line of symmetry has order 2~~
∴ Max. order of any elt. of $D_3 = 3$.
||'ly, ——— $D_4 = 4$

∴ Max order of any elt. of $D_3 \oplus D_4 = \text{lcm}(3,4) = 12$.

∴ There is no. elt. of order 24 in $D_3 \oplus D_4 \Rightarrow D_{24} \not\cong D_3 \oplus D_4$.

36) Suppose G is a group of order 4 and $x^2 = e$ for $x \in G$. Prove that G is isomorphic to $Z_2 \oplus Z_2$.

Page No. 105
Date

Pf: $x \in G$, & $x^2 = e \ \forall x \in G$.
$\Rightarrow x = x^{-1}$
If every elt. is its own inverse then G is abelian.
Now, G is a finite abelian grp. of order 4.
$\Rightarrow G \approx Z_4$ or $G \approx Z_2 \oplus Z_2$.
Now, Z_4 has an elt. of order 4.
But G has no. elt. of order 4.
$\Rightarrow G \not\approx Z_4$
$\therefore G \approx Z_2 \oplus Z_2$.

Q. 40 Express U(165) as an EDP of cyclic additive grps. of the form Z_n

Ans
$U(165) = U(3.5.11)$ $\quad U(st) \approx U(s) \oplus U(t) \Leftrightarrow (s,t) = 1$
$\Rightarrow U(165) \approx U(3) \oplus U(5) \oplus U(11)$
Also, $U(p^n) \approx Z_{p^n - p^{n-1}}$
$U(165) = Z_{3^1-3^0} \oplus Z_{5^1-5^0} \oplus Z_{11^1-11^0}$
$= Z_2 \oplus Z_4 \oplus Z_{10}$

Q.41 Express U(165) as an EDP of U-groups.
$U(165) = U(3.5.11) = U(3) \oplus U(5) \oplus U(11)$
$= U(15) \oplus U(11)$
$= U(33) \oplus U(5)$

* * *

Some Useful Links:

1. **Free Maths Study Materials (**https://pkalika.in/2020/04/06/free-maths-study-materials/**)**

2. **BSc/MSc Free Study Materials (**https://pkalika.in/2019/10/14/study-material/**)**

3. **MSc Entrance Exam Que. Paper: (**https://pkalika.in/2020/04/03/msc-entrance-exam-paper/**)**
   [JAM(MA), JAM(MS), BHU, CUCET, ...etc]

4. **PhD Entrance Exam Que. Paper: (**https://pkalika.in/que-papers-collection/**)**
   [CSIR-NET, GATE(MA), BHU, CUCET,IIT, NBHM, ...etc]

5. **CSIR-NET Maths Que. Paper: (**https://pkalika.in/2020/03/30/csir-net-previous-yr-papers/**)**
   [Upto 2019 Dec]