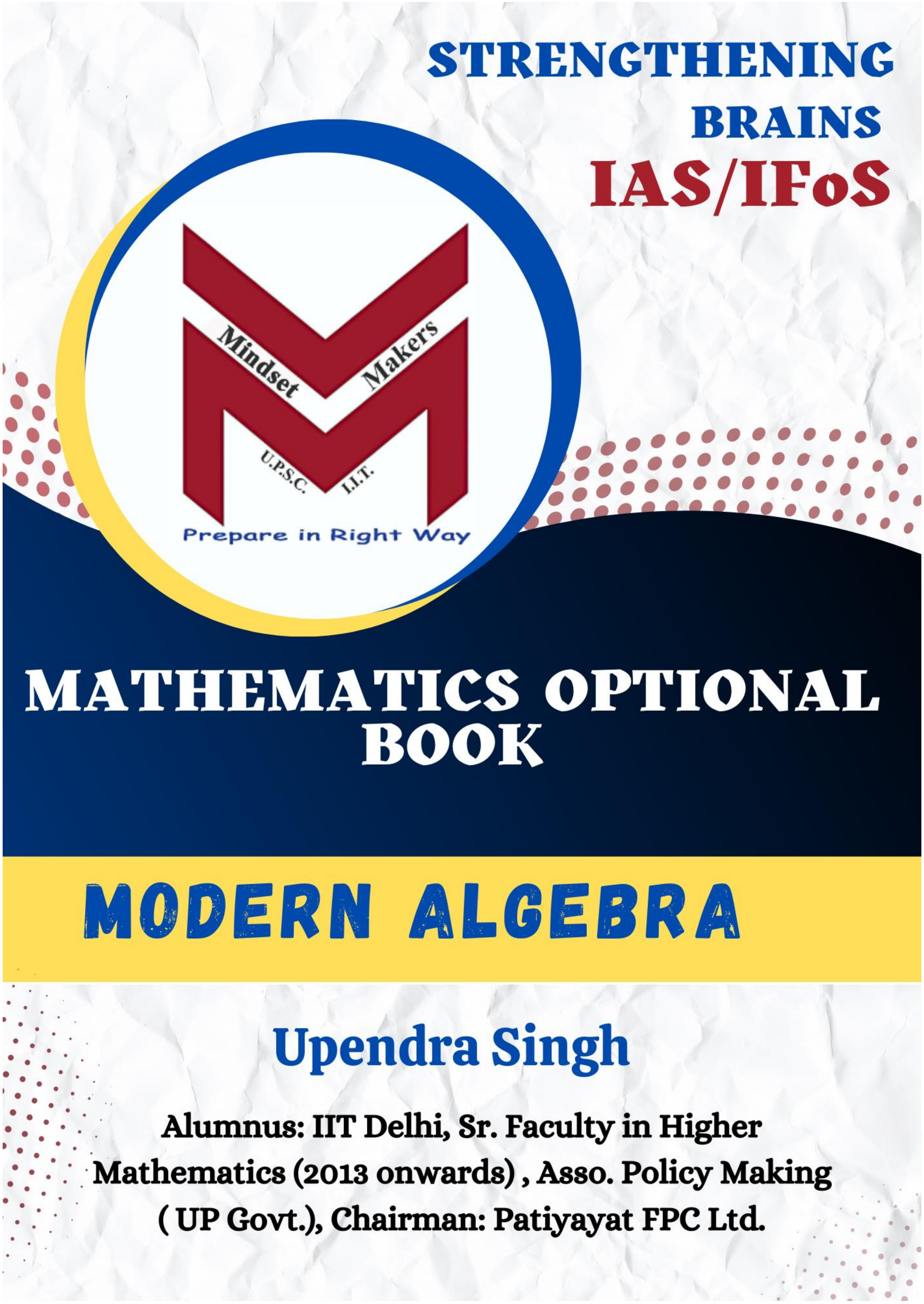

STRENGTHENING
BRAINS
IAS/IFoS
Mindset Makers
U.P.S.C. I.I.T.
Prepare in Right Way
MATHEMATICS OPTIONAL BOOK
MODERN ALGEBRA
Upendra Singh
Alumnus: IIT Delhi, Sr. Faculty in Higher Mathematics (2013 onwards) , Asso. Policy Making (UP Govt.), Chairman: Patiyayat FPC Ltd.


WELL PLANNED COURSE BOOK BASED ON DEMAND OF UPSC CSE IAS/IFOS :
01 Conceptual Development
02 Problem Solving Techniques
03 Assignments
04 Chapter wise PYQs Analysis
05 Test
MINDSET MAKERS
I.I.T UPSC

Mindset Making for Modern Algebra-

(Following brain storming will precisely give a feel to Aspirants that What's the outline of this topic)

Preliminaries: [Introduction]

- Number systems, properties of number systems
- Modular arithmetic
- Mathematical induction
- Equivalence Relations, functions

Modern Algebra-Group Theory :
Part (a)

- Set theory, binary composition, algebraic structure
- Closure, associative, identity, inverse commutative axioms-group-abelian group.
- Understanding & visualizing some famous groups
- Infinite groups
  $C, \mathbf{R}, Q, Z, mZ$
  $C^*, \mathbf{R}^*, \mathbf{Q}^*, \mathbf{C}\times\mathbf{R}, \mathbf{C}\times\mathbf{R}, ...$
  $GL_n(\mathbf{R}), SL_n(\mathbf{R})$ etc.
- Finite groups: Roots of unity, $Z_n, K_4,$
  $Q_8, S_n, D_n, GL_n(Z_p), SL_n(Z_p)$

Part (b)

- Subgroups, one step subgroup test, visualizing subgroups for all famous groups.
- Cyclic groups
- Order of a group, order of elements of a group, generators, finding number of elements of some given possible order in a famous group.
- Concept of Isomorphism (Visualizing), Cayley's theorem finite cyclic groups and Z_n. Extend Direct product $Z_m \times Z_n \approx Z_{mn}$!! ?

Part (c):

- Co-sets and Lagrange's theorem, Fermat's principle
- Normal subgroups and factor groups (visualization through Q/Z different examples of normal subgroups of famous groups.
- Grow Homomorphism: $G | \ker\phi \approx \operatorname{Im}\phi$, finding possible no of homomorphism from $G_1 \to G_2$
- Fundamental theorem of finite Abelian groups

Part (d):
Some special Topics:
Sylow Theorems: Conjugacy classes, The class equation, Cauchy's theorem, Application of Sylow theorems, Simple Groups

- Product of subgroups of a group
- Groups of order upto 15 of order pq where p and q are primes.

Equivalence relation on a set

A binary relation $\sim$ on a set X is said to be an equivalence relation, if and only if it is reflexive, symmetric and transitive. That is, for all a, b and c in X :

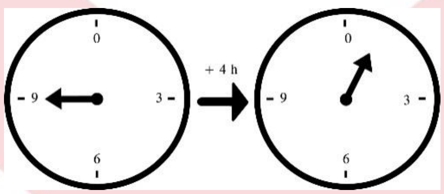
- $a \sim a$ (reflexivity) means each element is related to itself.
- $a \sim b$ if and only if $b \sim a$ (symmetry)
- If $a \sim b$ and $b \sim c$ then $a \sim c$ (transitivity)

X together with the relation $\sim$ is called a setoid.

The equivalence class of a under $\sim$, denoted $[a]$, is defined as $[a] = \{x \in X : x \sim a\}$ = collection of all those elements of X which are related to element a by the given relation.

Modular arithmetic-

In mathematics, modular arithmetic is a system of arithmetic for integers, where number "wrap around" when reaching a certain value, called the modulus. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book Disquisitiones Arithmetices, published in 1801.



Time- keeping on this clock use arithmetic modulo 12. Adding 4 hours to 9o'clock gives 1 o'clock, since 13 is congruent to 1 modulo 12.

A familiar use of modular arithmetic is in the 12 hours clock, in which the day is divided into two 12 hours periods. If the time is 7:00 now, then 8 hours later it will be 3:00. Simple addition would result in $7+8=15$, but clock wrap around" every 12 hours. Because the hour number starts over at zero when it reaches 12, this is arithmetic modulo 12. In terms of the definition below,15 is congruent to 3 modulo 12, so "15:00" on a 24-hour clock is displayed "3:00" on a 12 hour clock.

Congruence:-

Given an integer $n > 1$, called a modulus, two integers a and b are said to be **congruent** modulo n. If n is divisor of their difference (that is, if there is an integer k such that $a - b = kn$)

Congruence modulo n is a congruence relation, meaning that it an equivalence relation that is compatible with the operations of addition, subtraction, and multiplication. Congruence modulo n is denotes.

$$a \equiv b \pmod{n}.$$

The parentheses mean that $(\bmod\, n)$ applies to the entire equation, not just to the right-hand side (here b). This notation is not be confused with the notation $b \bmod n$ (without parentheses), which refers to the modulo operation. Indeed b mod n denoted the unique integer a such that $0 \le a < n$ and $a \equiv b \pmod{n}$ (that is, the remainder of b when divided by n)

The congruence relation may be rewritten as $a = kn + b$, explicitly showing its relationship with Euclidean division. However, the b here need not be the remainder of the division of a by n. Instead, what the statements $a \equiv b \pmod{n}$ asserts is that a and b have the same remainder when divided by n. That is

$a = pn + r$,

$b = qn + r$, where $0 \le r < n$ is the common remainder.

Subtracting these two expression, we recover the previous relation:

$a-b=kn$ by setting $k=p-q$

Example:- In modulus 12, one can assert that $38\equiv 14(\mathrm{mod}\,12)$ because $38-14=24$, which is a multiple of 12. Another way to express this is to say that both 38 and 14 have the same remainder 2, when divided by 12.

The definition of congruence also applies to negative values. For example:

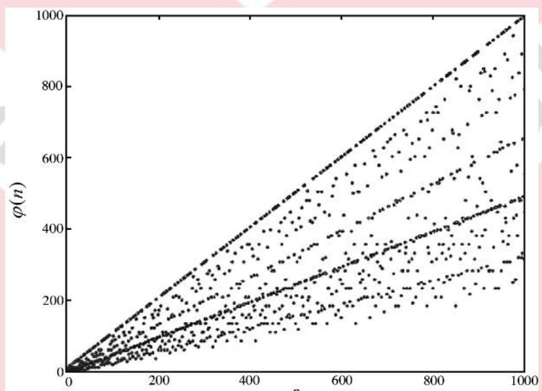
$$2\equiv -3(\mathrm{mod}\,5)$$

$$-8\equiv 7(\mathrm{mod}\,5)$$

$$-3\equiv -8(\mathrm{mod}\,5)$$

Euler's totient function-

In number theory, **Euler's totient function** count the positive integers up to a given integer n that are relatively prime to n, it is written using the. Greek letter phi as $\varphi(n)$ or $\phi(n)$, and may also be called **Euler's phi function.** In other wards, it is the number of integer k in the range $1\le k\le n$ for which the greatest common divisor $\gcd(n,k)$ is equal to 1.[2][3]. The integer k of this form are sometimes referred to as totatives of n.



The first thousand value of $\varphi(n)$. The points on the top line represent $\varphi(p)$ when p is a prime number, which is $p-1$[1]

For example, the totative of $n=9$ are the six number 1,2,4,5,7 and 8. They are all relatively prime to 9, but the other three numbers in this range 3,6, and 9 are not, since $\gcd(9,3)=\gcd(9,6)=3$ and $\gcd(9,9)=9$. Therefore $\varphi(9)=6$. As another example $\varphi(1)=1$ since for $n=1$ the only integer in the range from 1 to n is 1 itself, and $\gcd(1,1)=1$.

Euler's totient function is a multiplicative function, meaning that if two numbers m and n are relatively. Prime, then $\varphi(mn)=\varphi(m)\varphi(n)$.[4][5]. This function given the order of the multiplicative group of integers modulo n (the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$). It is also used to defining the RSA encryption system.

Mathematical induction is a method for proving that a statement is true for every natural number, that is, that the infinitely many cases all hold. Informal metaphors help to explain this technique, such as falling dominoes or climbing a ladder:

Mathematical induction proves that we can climb as high as we like on a ladder, by proving that we can climb onto the bottom rung (the **basis**) and that from each rung we can climb up to the next one (the **step**).

A **proof by induction** consists of two cases. The first, the **base case**, proves the statement for without assuming any knowledge of other cases. The second case, the **induction step**, proves that *if* the statement holds for any given case , *then* it must also hold for the next case. These two steps establish that the statement holds for every natural number . The base case does not necessarily begin with , but often with , and possibly with any fixed natural number, establishing the truth of the statement for all natural numbers.

Group Definition: Let G be a non-empty set and "O" is any binary operation $(G \quad 0)$ is called Group if it satisfies following properties:

1. Closure property $\forall a \in G, \forall b \in G \Rightarrow aob \in G$
2. Associative
   $ao(boc) = (aob)oc \forall a,b,c \in G$
3. Identity:
   $\forall a \in G, \exists e \in G$ s.t. $aoe = eoa = a$
4. Inverse
   For **each** $a \in G \ \exists \ a^{-1} \in G$ s.t.
   $aoa^{-1} = a^{-1}oa = e$

A group G is said to be abelian group if $ab = ba$, $\forall \quad a,b \in G$

Order of Group: Number of Elements in group G is called Order or Group G, it is denoted by $O(G) = |G|$

<u>**Assignment # 1**</u>

CATEGORY- A

Q1. Give two reasons why set of odd integers is not a group under addition.

$\because$ Set of integers $G = \{......2, -1, 0, 1, 2, 3, ...\}$

Set odd integers $G' = \{...... -3, -1, 1, 3, 5, 7, ...\}$

$(G', +)$ is not a group Reason (i) Not closed Reason (ii) Not having identity

Explanation: $\because -1 + 1 = 0 \notin G'$

Q2. $\{(Q+), (R+)(C+)\}$ $\rightarrow$ Group with Identity 0 and inverse of $a = -a$.

- Is $(N+)$ a group? Ans. No, Identity 0 does not belong to N.
- $S = N \cup \{0\}$. Is $(S+)$ a group? Ans. No, $2 \in S$ but $-2 \notin S$ s.t. $2 + (-2) = 0$
- $\left.\begin{array}{l}(\mathbf{Q}^*) \\ (\mathbf{R}^*) \\ (\mathbf{C}^*)\end{array}\right\}$ is a group w.r.t usual multiplication with Identity 1 with inverse of a $= \frac{1}{a}$?
- $Z - \{0\}$ is a group w.r.t usual multiplication?

Ans. No. because $3 \in Z - \{0\}$ but $\frac{1}{3} \notin Z - \{0\}$ s.t. $3 \times \frac{1}{3} = 1$

- $(Z+)$ is an abelian group? **Solution**: Yes, $a+b=b+a$, $\forall a,b\in Z$. Moreover $(Q,+),(\mathbf{R}+),(\mathbf{C}+),(Q^*,.),(\mathbf{R}+),(\mathbf{C}^*,.)$ are abelian groups.

(b) Why subtraction is not associative?

$\because a-(b-c)=a-b+c$; $(a-b)-c=a-b-c$. clearly $a-(b-c)\neq(a-b)-c$

Q3. $G=\mathbf{Z}$ & $aob=a+b+1,\ a,b\in Z$ then (G,o) forms an group ?

Solution: (1) $\forall a\in Z,\ \forall b\in Z\,; aob=a+b+1\in Z\ \ \therefore aob\in Z,\ \forall a,b\in Z$

(2) Associative $a\circ(b\circ c)=(a\circ b)\circ c$

L.H.S. = $a\circ(b\circ c)=a\circ(b+c+1)=a+(b+c+1)+1=a+b+c+2$

R.H.S. $(a\circ b)\circ c=(a+b+1)\circ c=(a+b+1)+c+1=a+b+c+2$

L.H.S.=R.H.S.

Hence, $a\circ(b\circ c)=(a\circ b)\circ c,\forall a,b,c\in Z$. Also we may think by that integers follow associativity.

(3) Identity let b is the identity of G then $a\circ b=a\Rightarrow \cancel{a}+b+1=\cancel{a}\ \Rightarrow b=-1$

(4) Inverse : Suppose b is the inverse of a then $a\circ b=-1;\ a+b+1=-1;\ b=-2-a$

Therefore $(G,0)$ is a group w.r.t given operation.

Q4. (i) $G=Q^+\rightarrow$ Set of all positive rational numbers s.t. $a\circ b=\frac{ab}{3}$ then (G,o) is group?

(ii) $G=Q^-\rightarrow$ Set of all negative rational number $a\circ b=\frac{ab}{3}$ then (G,o) is group?

Ans. (ii) Not a group $-1\in Q^-$ $(-1)o(-2)=\frac{(-1)(-2)}{3}=\frac{2}{3}\notin Q^-$. Hence $(G,0)$ is not a group

(i) $a\circ b=\frac{ab}{3}$. So $(a\circ b)\circ c=a\circ(b\circ c)$ implies $\frac{ab}{3}\circ c=a\circ(b\circ c)$; $\frac{ab}{3}\circ c=a\circ\frac{bc}{3}$; $\frac{abc}{9}=\frac{abc}{9}$

i.e. if $a=1,\ b=3;\ a\circ b=\frac{ab}{3};\ 1\circ 3=\frac{\cancel{3}}{\cancel{3}}=1\notin Q^+$

It is not a group.

CATEGORY- B

Q5. For $\alpha,\beta\in\mathbf{R}$ define the map $\phi_{(\alpha,\beta)}:\mathbf{R}\rightarrow\mathbf{R}$ by $\phi_{(\alpha,\beta)}(x)=\alpha x+\beta$. Let $G=\{\phi_{\alpha,\beta}:(\alpha,\beta)\in\mathbf{R}^2\}$. For $f,g\in G$ define $g\circ f\in G$ by $(g\circ f)(x)=g(f(x))$. Then discuss about closure, associative, identity and inverse axiom of elements of G.

- G is the collection of functions and we know that composition of functions $(g\circ f)(x)g(f(x))$ is associative. So $(G,\circ)$ satisfies associative axion.
- Closure: Let $f=\phi_{\alpha,\beta},g=\phi_{\gamma_1\delta}$ then

$(g\circ f)(x)=g(f(x))=\phi_{\gamma,\delta}(\alpha x+\beta)=\gamma(\alpha x+\beta)+\delta=(\gamma\alpha)x+(\gamma\beta+\delta)$

$(g\circ f)(x)=cx+d$ where $c,d\in\mathbf{R}\Rightarrow g\circ f\in G\therefore(G_0)$ is closed.

Identity: Let if $\exists\ I\in G$ s.t. $f\circ I=f;\ \forall f\in G$

$f(I(x))=f(x)$

$\because$ We wish to have now think!!

$\phi_{\alpha,\beta}\circ\phi_{\gamma\delta}=\phi_{\alpha,\beta}$; $\phi_{\alpha,\beta}(\gamma x+\delta)=\phi_{\alpha,\beta}(x)\Rightarrow\alpha(\gamma x+\delta)+\beta=\alpha x+\beta\Rightarrow\gamma=1,\delta=0$

$\boxed{I=\phi_{(1,0)}}$. So $\phi_{(1,0)}$ works as an identity element of $(G,0)$

Inverse axiom: Let $\phi_{(\alpha,\beta)}\cdot\phi_{(\gamma,\delta)}=\phi_{(1,0)}\Rightarrow\phi_{\alpha,\beta}(\gamma x+\delta)=1\cdot x+0\Rightarrow\alpha(\gamma x+\delta)+\beta=1\cdot x$

$\Rightarrow\alpha\cdot\gamma=1,\ \alpha\cdot\delta=0,\ \beta=0$ which fails to exist for $\alpha>0\therefore(G,0)$ does not satisfy inverse axiom.

$\therefore(G,0)$ is not a group.

Commutative: Commutativity need not be satisfied for composition of functions.

(c) Let $G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$ of six transforms on the set of Complex number defined by

$f_1(z)=z,\ f_2(z)=1-z,\ f_3(z)=\dfrac{z}{(z-1)},$

$f_4(z)=\dfrac{1}{z},\ f_5(z)=\dfrac{1}{1-z},\ f_6(z)=\dfrac{(z-1)}{z}$

- What do you understand by composition of functions?
- The given set G is closed w.r.t. composition of functions?
- Composition of two functions *f* and *g* is defined as $(f\circ g)(x)=f(g(x))$ where *f* is a function defined on some non-empty $A\to B$ and $g:C\to A$
- Example to understand $f\circ g$ for given set G,

$$(f_1\circ f_2)(z)=f_1(f_2(z))=f_1(1-z)=1-z=f_2(z)$$

$$(f_6\circ f_5)(z)=f_6(f_5(z))=f_6\left(\frac{1}{1-z}\right)=\frac{\frac{1}{1-z}-1}{\frac{1}{1-z}}=\frac{z}{(1-z)}(1-z)=z=f_1(z)$$

$$(f_3\circ f_4)(z)=f_3(f_4(z))=f_3\left(\frac{1}{z}\right)=\frac{1/z}{\left(\frac{1}{z}-1\right)}=\frac{1}{z}\times\frac{z}{(1-z)}=\frac{1}{(1-z)}=f_5(z)$$

$$(f_1\circ f_3)(z)=f_1(f_3(z))=f_1\left(\frac{z}{z-1}\right)=\frac{z}{z-1}=f_3(z),$$

$$(f_1\circ f_4)(z)=f_1(f_4(z))=f_1\left(\frac{1}{z}\right)=\frac{1}{z}=f_4(z),\ (f_1\circ f_5)(z)=f_1(f_5(z))=f_1\left(\frac{1}{1-z}\right)=f_5(z)$$

$$(f_1\circ f_6)(z)=f_1(f_6(z))=f_1\left(\frac{z-1}{z}\right)=\frac{z-1}{z}=f_6(z)$$

Observations: Composition of any function with $f_1(z)$ gives that function itself.

$f_6 \circ f_5 = f_1$ implies inverse kind thought.

Note: As the given set has finite number of elements so we can try to compose all possibilities in a **Cayley table.**

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_3	f_6	f_4
f_3						
f_4						
f_5						
f_6						

Now observe Cayley table for closure, Associative identity, inverse.
Composition of functions need not be commutative (Example $f_2 \circ f_3 \neq f_3 \circ f_2$)

Exam point:
While composing functions for Cayley table, you may feel to quit. But if you have feeling for 'How to compose functions' you can do those easily by just observing function. (So don't quit as its easy). After just two revisions, you will have good command over it. It helps you in taking edge over others because in algebra; we have to do these compositions repeatedly. (It will come into your habit). (These are standard examples, so they ask questions by just changing representations on same questions).

CATEGORY- C

Q(6). Show that Quartennion (Q_4) is a group with respect to multiplication

$$Q_4 = \{\pm i, \pm + j, + j, +k \mid i^2 = j^2 = k^2 = -1, ij = ji = k, jk = kj = 1, ki = ik = j\}$$

Ans.
(1) From Table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	k	j	j
$-i$	$-i$	i	1	-1	k	k	j	j
j	j	$-j$	k	k	-1	1		1
$-j$	$-j$	j	k	k	1	-1	1	1
k	1	$-k$	j	j	1	1	-1	1
$-k$	$-k$	k	j	j	1	1	1	-1

(2) Associative law; $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall a, b, c \in Q_4$

(3) $\forall a \in Q_4, \ \exists\, 1 \in Q_4$ s.t. $a \cdot 1 = 1 \cdot a = a$

(4) Inverse of each element of Q_4; $1^{-1}=1, -1=-1, i^{-1}=-i, (-i)^{1}=i, (j)^{-1}=-j, (-j)^{-1}=-j$,

$(k)^{-1}=-k, (-k)^{-1}=k$

Thus Q_4 is group w.r.t. multiplication

$Q_4=\{\pm 1, \pm i, \pm j, \pm k\}$ is it abelian? **Solution: No;** $i \in Q_4$, $j \in Q_4$, $ij = k \neq ji$ then

CATEGORY- D

How you differentiate?

- $\mathbf{Z}_n$ and Z
- $\mathbf{Z}_n$ and $\mathbf{Z}_m$
- $\mathbf{Z}_m$ and $m\mathbf{Z}$

Also write about how they form group?

- $\mathbf{Z}_n$ represents modulo *n* whereas $\mathbf{Z}$ represents set of integers. $\mathbf{Z}_n$ is a finite set with elements as classes and $\mathbf{Z}$ is an infinite set.

$\mathbf{Z}_n=\{[0],[1],[2],....[(n-1)]\}$

$\mathbf{Z}_m=\{[0],[1],[2],....[(m-1)]\}$

$\mathbf{Z}=\{.......-3,-2,-1,0,1,2,......\}$

$2\mathbf{Z}=\{......-4,-2,0,2,4,6,.....\}$: set of even integers

$m\mathbf{Z}=\{......3m,-2m,-m,0,m,2m,......\}$

Set of integers in multiple of *m*.

- $\mathbf{Z}, m\mathbf{Z}$ are groups w.r.t. usual addition.
- $\mathbf{Z}_n$ forms a group w.r.t. addition modulo *n*.
- $\mathbf{Z}_n^*$; where *p* is a prime number and collection of non-zero classes in modulo *p* forms a group w.r.t. multiplication modulo.

Examples to feel:

$\mathbf{Z}_4=\{[0],[1],[2],[3]\}$ is a group w.r.t. addition modulo 4 but not a group w.r.t. multiplication modulo 4 (composite numbers cannot fulfill demand of group axioms).

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Observe both Cayley tables 1 may seem as an identity element w.r.t. multiplication modulo $4(\cdot 4)$. Then what about inverse of element O? (Does not exist.)

$\times_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Clearly O is out of the set of non-zero elements of modulo 4. So not closed.

Now let's observe $\mathbf{Z}_5^*$ forms a group w.r.t. multiplication modulo 5 (5 is a prime number).

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

CATEGORY- E

Can you try to differentiate two groups G_1 and G_2 ; where

G_1 = collection of all 2×3 matrices with real entries

G_2 = collection of all 2×2 matrices with real entries and with non-zero determinant.

G_1 does not form a group w.r.t matrix multiplication but forms a group w.r.t matrix addition.

G_2 does not form a group w.r.t matrix addition but forms a group w.r.t matrix multiplication.

Q. Show that $GL_n(\mathbf{F})$ is a group under multiplication?

Ans. Proof:

$GL_n(\mathbf{F}) = \left\{ A = \left[a_{ij} \right]_{n\times n} \middle| |A| \neq 0, a_{ij} \in \mathbf{F} \right\}$

(1) $A \in G_n(\mathbf{F}),\ B \in GL_n(\mathbf{F})$ s.t. $|A| \neq 0$ & $|B| \neq 0$. So $|A\cdot B| = |A|\cdot|B| \neq 0$.Then $A\cdot B \in GL_n(\mathbf{F})$

(2) $A\cdot(B\cdot C) = (A\cdot B)\cdot C,\ \forall A, B, C \in GL_n(\mathbf{F})$

(3) $\forall A \in GL_n(\mathbf{F}),\ \exists\ T_n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{n\times n} \in GL_n(\mathbf{F})$ s.t $A\cdot In = A = InA$

(4) $A \in GL_n(\mathbf{F}) \Rightarrow |A| \neq 0$ then $A^{-1} = \dfrac{adjA}{|A|}$; $\left|A^{-1}\right| = \dfrac{1}{|A|}$, since $|A| \neq 0$ then $\left|A^{-1}\right| \neq 0$

Therefore, $GL_n(\mathbf{F})$ is group under multiplication.

Q. Show that $SLn(\mathbf{F})$ is a group under multiplication?

Proof:

$SL_n(\mathbf{F}) = \left\{ A = \left[a_{ij} \right]_{n\times n} \middle| |A| = 1,\ a_{ij} \in \mathbf{F} \right\}$

(1) $A \in SL_n(\mathbf{F}),\ B \in SL_n(\mathbf{F})$ s.t $|A| = 1$ & $|B| = 1$

$|A\cdot B| = |A|\cdot|B| = 1$, Then $A\cdot B \in SL_n(\mathbf{F})$

(2) $A\cdot(B\cdot C)=(A\cdot B)\cdot C\,\forall A,B,C\in GL_n(\mathbf{F})$

(3) $\forall A\in SL_n(\mathbf{F}),\ \exists,\ In=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}_{n\times n}\in SL_n(\mathbf{F})$ s.t $A\cdot I_n=A=I_n\cdot A$

(4) $A\in SL_n(\mathbf{F})\Rightarrow |A|=1$, then $A^{-1}=\dfrac{adjA}{|A|}$ $|A^{-1}|=\dfrac{1}{|A|}$ since $|A|=1$ then $|A^{-1}|=1$

Therefore, $SL_n(\mathbf{F})$ is group under multiplication.

Q. $GL_n(\mathbf{F})$ is abelian? Ans. Need not be abelian. **If** $n=1$ then $GL_n(\mathbf{F})=\left\{A=\left[a_{ij}\right]_{1\times1}\middle|\,|A|\neq 0, a_{ij}\in 11\right\}$

Suppose $\mathbf{F}=\mathbf{R}$ then $GL_n(\mathbf{R})=\left\{A=[a]\middle|\,|A|\neq 0, a\in\mathbf{R}\right\}=\mathbf{R}^*$

$\mathbf{R}^*$ is abelian group w.r.t multiplication then $GL_1(\mathbf{R}^*)$ is abelian group of order ∞.

If $n\geq 2$ then $GL_n(\mathbf{F})$ is non-abelian group.

Q. $SL_n(\mathbf{F})$ is an abelian group?

Ans. (i) If $n=1$ then $SL_n(\mathbf{F})$ is abelian (ii) If $n\geq 2$ then $SL_n(\mathbf{F})$ is non-abelian.

Q. Find total number of elements in $GL_2(\mathbf{R})$ and $GL_2(\mathbf{Z}_5)$.

NOTE: $\mathbf{Z}_5$ is a field. So entries of general linear group (which come from some field) contains here those matrices which has entries from the field $\mathbf{Z}_5$ and with non-zero determinant.

$GL_2(\mathbf{R})=\left\{\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix},.....\right\}$; Infinite number of elements

$GL_2(\mathbf{Z}_5)=\left\{\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix},\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\begin{bmatrix}2 & 3\\ 0 & 3\end{bmatrix},.....\right\}$; (Just keep in mind non-zero determinant)

NOTE: For the general linear group with entries from finite field; we think like

$\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\begin{matrix}\to \text{Row 1 has } 5\times5-1 \text{ choices}\\ \to \text{Row 2 has } 5\times5-5 \text{ choices}\end{matrix}$

$\therefore$ Total number of elements in $GL_2(\mathbf{Z}_5)$ are $=(5^2-1)(5^2-5)=24\times20=480$

Exam Point:

In general $\left|GL_n(\mathbf{Z}_p)\right|=(p^n-1)(p^n-p)(p^n-p^n)....(p^n-p^{n-1})$

$$\left|SL_n(\mathbf{Z}_p)\right|=\frac{(p^n-1)(p^n-p)....(p^n-p^{n-1})}{p-1}$$

Q. Find the inverse of the element $\begin{bmatrix}2 & 6\\ 3 & 5\end{bmatrix}$ in $GL_2(\mathbf{Z}_{11})$.

Let $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in GL_2(\mathbf{Z}_{11})$ s.t. $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ [Property of inverse]

$$\Rightarrow \left.\begin{matrix} 2\alpha + 6\gamma = 1 \;\; ....(1) \\ 2\beta + 6\delta = 0 \;\; ...(2) \\ 3\alpha + 5\gamma = 0.......(3) \\ 3\beta + 5\delta = 1.......(4) \end{matrix}\right] \rightarrow \text{System of linear equations in unknown } \alpha, \beta, \gamma, \delta .$$

$\therefore$ Solve this system and get $\alpha, \beta, \gamma, \delta$ (Note that $\alpha, \beta, \gamma, \delta$ are elements of $\mathbf{Z}_{11}$).
How!! (Now you go by hit & trial)
Let's choose $\alpha = 3, \gamma = 1$
Satisfy (1) but not (3) cannot work.
(looking bit tricky!!)

Let's try to solve equations (1) and (3); $2\alpha + 6\left(\frac{-3}{5}\alpha\right) = 1 \therefore 2\alpha + 6(-3\times 9\alpha) = 1$; $2\alpha - 282\alpha = 1$

$2\alpha - 7\alpha = 1;\ -5\alpha = 1;\ 6\alpha = 1 \Rightarrow \alpha$ = inverse of 6 in $\mathbf{Z}_{11} = 2$.

Here $\frac{1}{5}$ represents inverse of 5 in $\mathbf{Z}_{11} = 9$; $5\cdot 1 = 1$ in mod 11 $\therefore \alpha = 2$ $\therefore$ From (1) $6\gamma = 1 - 4 = -3 = 8$

$\therefore \gamma = \frac{8}{6} = 8\times 2 = 16 = 5$

Now Similarly we can solve equation (1) and (4) $\because$ $3\beta + 5\left(-\frac{2}{6}\beta\right) = 1$; $3\beta - 20\beta = 1$; $= 17\beta = 1$

$5\beta = 1 \Rightarrow \beta = \frac{1}{5} = 9 \therefore$ $6\delta = -2\times 9 = -18 = 4$

$\delta = \frac{4}{6} = 4\times 2 = 0 \therefore$ Required element is $\begin{bmatrix} 2 & 9 \\ 5 & 8 \end{bmatrix}$.

Q. $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| O \neq a \in \mathbf{R} \right\}$ is group w.r.t multiplication?

Ans. $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| a \neq 0 \in \mathbf{R} \right\}$

(1) $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G,\ B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$; $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$

(2) Associative law; $A\cdot(B\cdot C) = (A\cdot B)\cdot C,\ \ \forall A, B, C \in G$ as Matrix multiplication follows associativity

(3) Let $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ is the Identity of G then $AB = A$

$\Rightarrow \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \Rightarrow \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \Rightarrow 2ab = a \Rightarrow b = \frac{1}{2}$ .So $B = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$ is the identity of G.

(4) Inverse: suppose $B=\begin{bmatrix} b & b \\ b & b \end{bmatrix}$ is inverse of $A=\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ Then $\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix}=\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}=\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \Rightarrow 2ab=\frac{1}{2};\ b=\frac{1}{4a},\ O\neq a\in\mathbf{R}$ .Then $B=\begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$

Therefore $G=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| O\neq G\in\mathbf{R}\right\}$ is group w.r.t multiplication.

Q. $G=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| 0\neq a\in\mathbf{R}\right\}$ is group w.r.t multiplication?

Ans. (1) Closure Property:Let $A=\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix},\ B=\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\in G$

$A\cdot B=\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}\in G$. Closure Property holds because $\forall\ a,b\neq 0\Rightarrow ab\neq 0\in\mathbf{R}$

(2) Associative: $A(BC)=(AB)C\ \ \forall A,B,C\in G$ as Matrix multiplication follows associativity.

(3) Identity

Let $B=\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\in G$ be the identity then $AB=A\Rightarrow\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\Rightarrow\begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$

$\Rightarrow ab=a\Rightarrow b=1$. So identity $B=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

(4) Inverse, let $B=\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ is the inverse of then $AB=I$

$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\Rightarrow\begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix};\ ab=1\Rightarrow b=1/a$. Inverse $A^{-1}=\begin{bmatrix} 1/a & 0 \\ 0 & 0 \end{bmatrix}$

Therefore he given set forms a group w.r.t usual multiplication of matrices.

CATEGORY- F

Q. Show that ***n*^th^ roots of unit**y can be represented on the circumference of a unit circle centered at origin. Can you observe the cyclic property here?

Examples to feel: (1) Cube roots of unity $z=1,\ \omega,\ \omega^2$ where $\omega=-\frac{1}{2}+\frac{i\sqrt{3}}{2},\ \omega^2=-\frac{1}{2}-\frac{i\sqrt{3}}{2}$

$z=x+iy$

(2) Fourth roots of unity $z=1,-1,i,-i$

Now let's think about n^{th} roots of unity; $z = \left\{ e^{ik\cdot\frac{2\pi}{n}}; k = 0,1,2,....,(n-1) \right\} = \left\{1, e^{i\theta}, e^{i\theta_2}, ...e^{i\theta_{n-1}}\right\}$

As we know that the complex number $z = |z| \cdot e^{i\theta}$ is representation in polar form of a complex number on the complex plane. Modulus is one here. These complex number can be represented on the circumference of a unit radius circle centered at origin. We can imagine about multiplication of elements of *z* here it may lead to group structure.

Exam Point:
This is very famous example and gives opportunities for different kind of question. So keep your basics clear about roots of unity.

CATEGORY- G

Q. Can you try to observe properties of a group with exactly four elements?
Let $G = \{a,b,c,d\}$ be a group.
Observation (i): One out of *a*, *b*, *c*, *d* will be working as ideality element.
Let $a = e$

Observation (ii): Inverse of a is a because a is an identity element.

Observation (iii)	
Possibility (1)	**Possibility (2)**
Each element of G is self inverse $\Downarrow$ $a^{-1} = a, b = b^{-1}, c = c^{-1}, d = d^{-1}$ Now try to think: $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ $\therefore$ for given G and this possibility $\because (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ (we know it) $\Rightarrow \alpha\beta = \beta\alpha \Rightarrow G$ is commutative / abelian group. $\therefore$ $(\alpha\beta) \in G$ $\therefore (\alpha\beta)^{-1} = \alpha\beta$	Only two elements of G are self inverse let $a = a^{-1}, d = d^{-1}$ then we must have $b^{-1} = c$ and $c^{-1} = b$. Again we can observe G is abelian.

Therefore a group with exactly four elements is always abelian.

Exam point:
Above reasoning, helpful in thinking about groups of even order. At least two elements are self inverse.

Klein's 4 – Group: It is denoted by K_4
$K_4 = \{e, a, b, ab | a^2 = e, b^2 = 2, ab = ba\}$
Proof: Closure Property:
$a \cdot (ab) = a^2 b = e$

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

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

(2) Associative $x(yz) = (xy)z \quad \forall \quad x, y, z \in K_4$

(3) $\forall x \in K_4 \Rightarrow e \in K_4$ s.t $x\cdot e = ex = x$

(4) Inverse of each element $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$; $(ab)^{-1} = (ab)^{-1}$

Hence, (K_4) from a group of order 4 with identity *e*.

CATEGORY- H

$U(n)$ **is the collection of relative primes to *n* and** $U(n)$ **forms a group w.r.t multiplication modulo *n*.**

Can you observe difference between U(8) and U(10)? Why they behave differently even through both have equal cardinality?

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

8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

10	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

In $U(8)$	In $U(10)$
$3\cdot 3 = 1$	$3\cdot 3\cdot 3\cdot 3 = 1$
$5\cdot 5 = 1$	$7\cdot 7\cdot 7\cdot 7 = 1$
$7\cdot 7 = 1$	$9\cdot 9\cdot 9\cdot 9 = 1$

CATEGORY-I

- **<u>Symmetric or Permutation Group</u>**:
- S_n ={ Set of all one-one onto mapping from set containing *n* elements to itself} and $O(S_n) = \lfloor n = n!$
- If set containing one element then $S_1 = \{I\}, f:\{1\} \to \{1\}$
- If set containing 2-elements then $f:\{1,2\} \to \{1,2\}$

$f_1(1) \to 1,\ f_1(2) \to 2$

$\Rightarrow f_1 = \begin{pmatrix} 1 & 2 \\ f(1) & f(2) \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = I$

- $S_n = \left\{ \begin{pmatrix} 1 & 2 \\ f_2(1) & f_1(2) \end{pmatrix} \begin{pmatrix} 1 & 2 \\ f_2(1) & f_2(2) \end{pmatrix} \right\}$

$f_2(1) \to 2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

$f_2(2) \to 1$

- If set containing 3-elements then $f\ \{1,2,3\} \to \{1,2,3\}$

$\left.\begin{array}{l} f_1(1) \Rightarrow 1 \\ f_1(2) \Rightarrow 2 \\ f_1(3) \Rightarrow 3 \end{array}\right\} f_1 = \begin{pmatrix} 1 & 2 & 3 \\ f_1(1) & f_1(2) & f_1(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1$

$\left.\begin{array}{l} f_2(1) \to 2 \\ f_2(2) \to 1 \\ f_2(3) \to 1 \end{array}\right\} f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2) \text{ or } (21)$

$\left.\begin{array}{l} f_3(1) \to 3 \\ f_3(2) \to 2 \\ f_3(3) \to 1 \end{array}\right\} f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3) \text{ or } (31)$

$\left.\begin{array}{l} f_4(1) \to 1 \\ f_4(2) \to 3 \\ f_4(3) \to 2 \end{array}\right\} f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3) \text{ or } (31)$

$\left.\begin{array}{l} f_4(1) \to 1 \\ f_4(2) \to 3 \\ f_4(3) \to 2 \end{array}\right\} f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3) \text{ or } (32)$

$\left.\begin{array}{l} f_5(1) \to 2 \\ f_5(2) \to 3 \\ f_5(3) \to 1 \end{array}\right\} f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 3)$

$\left.\begin{array}{l} f_6(1) \to 3 \\ f_6(2) \to 1 \\ f_6(3) \to 2 \end{array}\right\} f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = (1\ \ 3\ \ 2)$

- **Definition**: Set of all one-one onto mapping from set containing *n* elements to itself forms a group under composition of functions. It is denoted by S_n and $O(S_n) = n!$ elements are called permutation of S_n.
- **Symmetric Group** S_1; $S = \{I\}$, $O(S_1) = 1$
- Group S_2; $S_2 = \{I, (1,2)\}$
- **Symmetric Group** S_3; $S_3 = \{I, (12), (13), (23), (123)(132)\}, O(S_3) = 6$

Dihedral Group (D_n): Group of Symmetries.

Note-

This group will not be asked directly but if you have idea about this group, then you can interpret many things about non abelian groups and some counter example kind of demands. Also this is a very famous group to feel the group structure practically. Let's enjoy.

$$D_n = \left\{ \begin{array}{l} x^i y^j \,\middle|\, x^2 = e, y^n = e, xy = y^{-1}x \\ \qquad \ell = 0,1 \quad y = 0,1,....n-1 \end{array} \right\}$$

$O(D_n) = 2n$

$x^i y^j$ is generator

$x^2 = e$ is Reflection

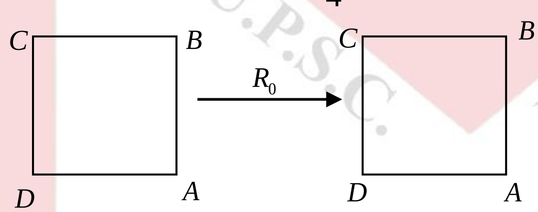
$x^2 = e, y^n = e$ is Relator

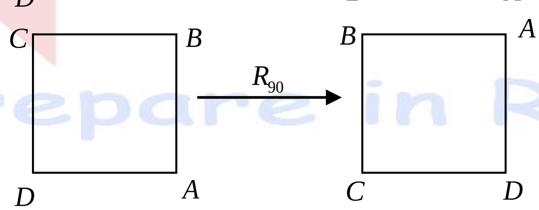
$xy = y^{-1}x$ is Relation

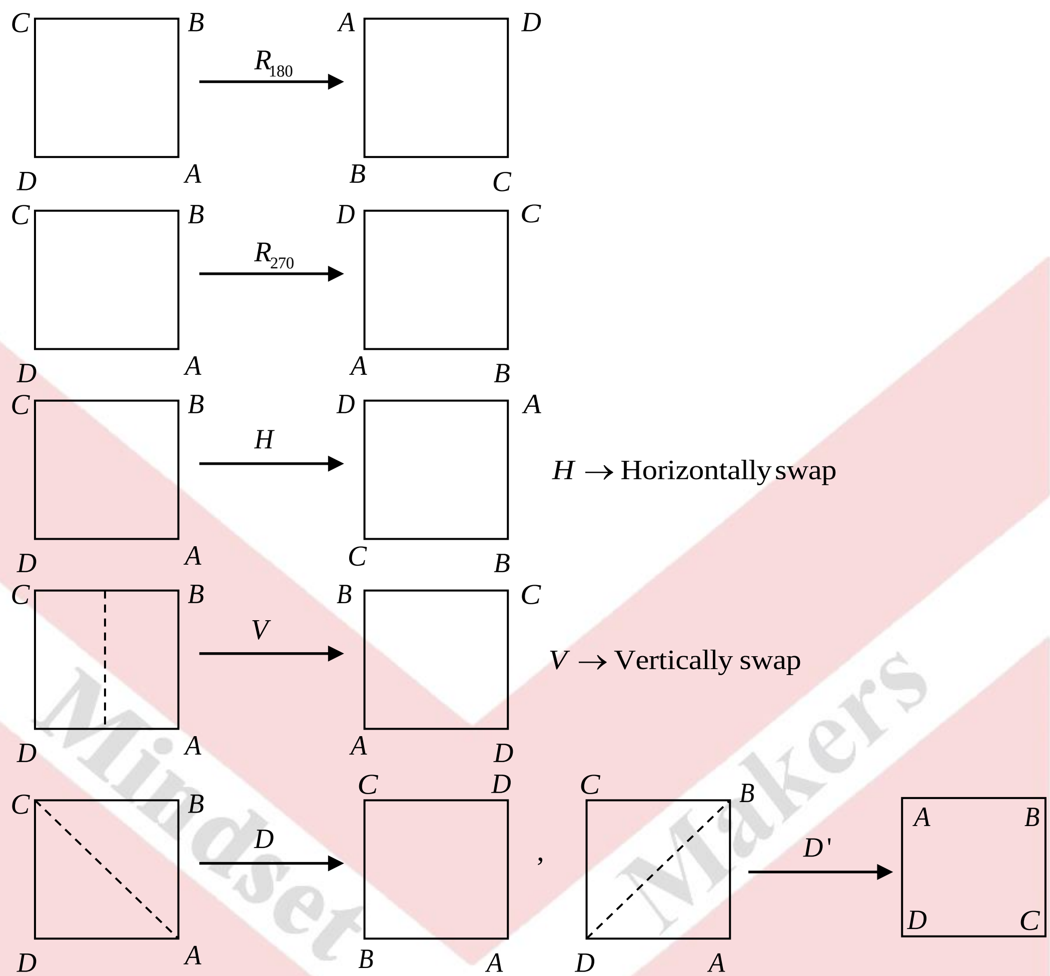
$y^n = e$ is Rotation

$$D_4 = \left\{ \begin{array}{l} x^i y^j \,\middle|\, x^2 = e,\ y^4 = e,\ xy = y^{-1}x \\ \qquad \ell = 0,1, \quad y = 0,1,2,3 \end{array} \right\}$$

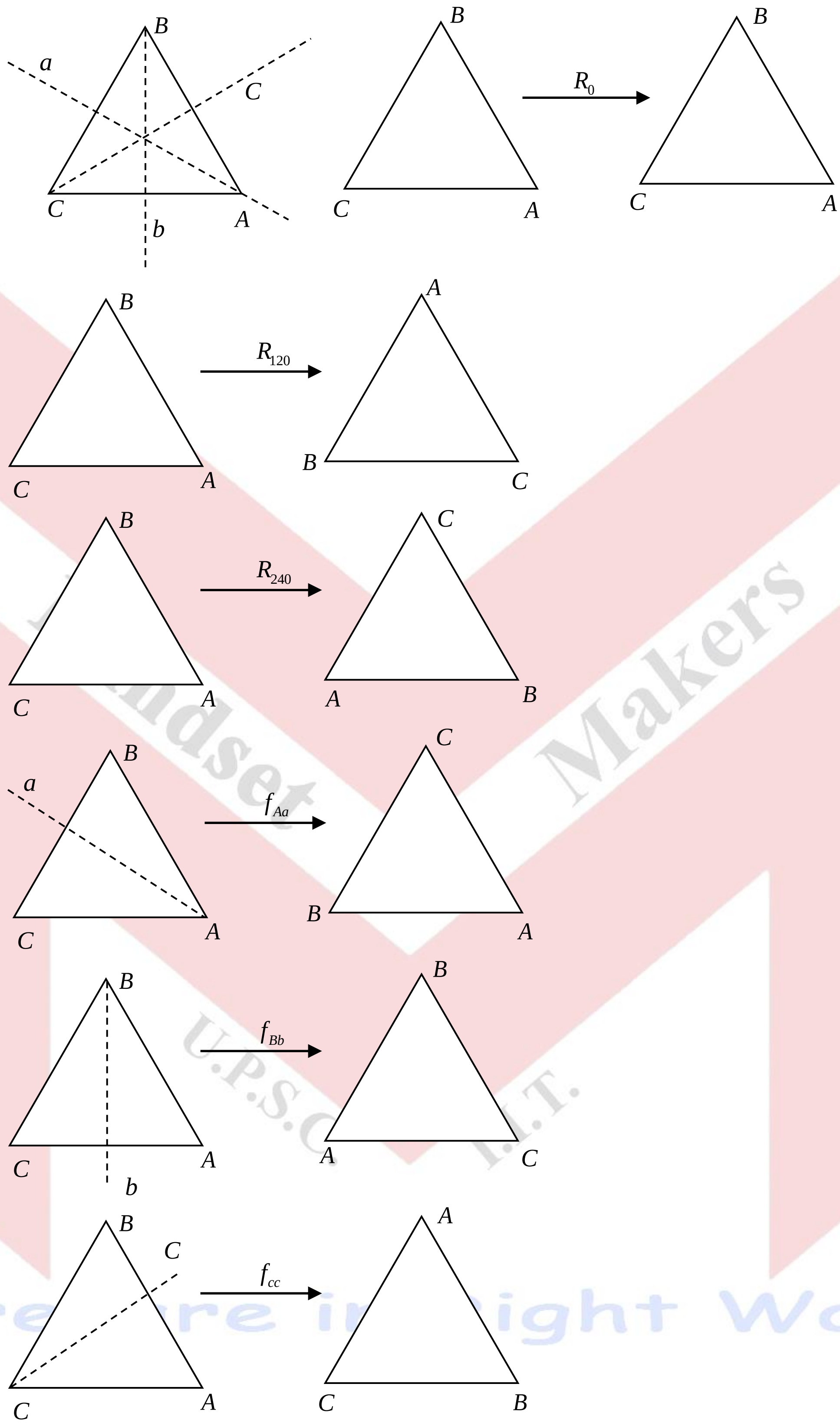
$O(D_4) = 2.4 = 8, \quad \theta = \frac{360°}{4} = 90°$





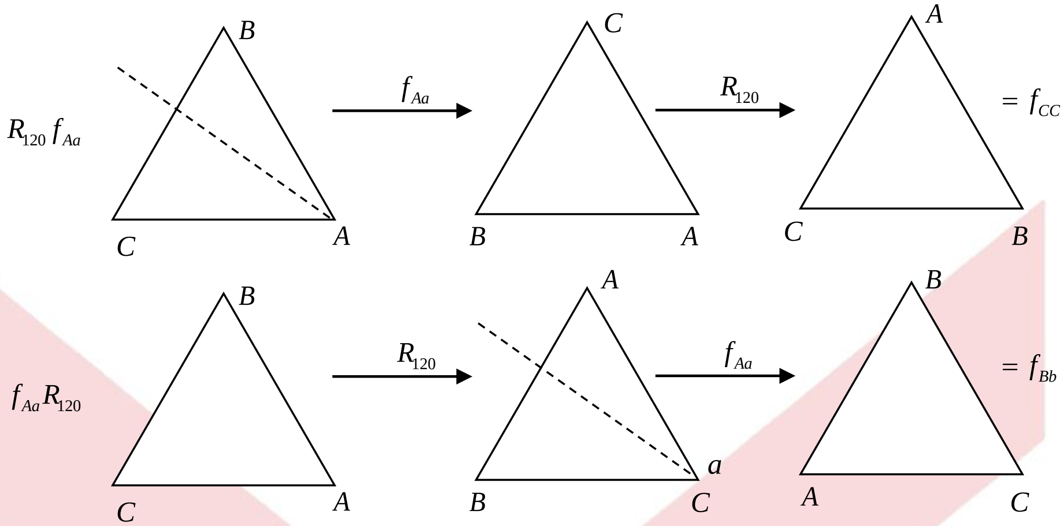


Equilateral Triangle



$D_3 = \left\{ R_0, R_{120}, R_{240,}\, f_{Aa}, f_{Bb}, f_{Cc} \right\}$

$R_{120}R_{240} = R_0 = R_{240}R_{120}$



$R_{120}\,f_{Aa} = f_{Cc}$

and $f_{Aa}R_{120} = f_{Bb}$

	R_0	R_{120}	R_{240}	f_{Aa}	f_{Bb}	f_{Cc}
R_0	R_0	R_{120}	R_{240}	f_{Aa}	f_{Bb}	f_{Cc}
R_{120}	R_{120}	R_{240}	R_0	f_{Cc}	f_{Aa}	f_{Bb}
R_{240}	R_{240}	R_0	R_{120}	f_{Bb}	f_{Cc}	f_{Aa}
f_{Aa}	f_{Aa}	f_{Bb}	f_{Cc}	R_0	R_{120}	R_{240}
f_{Bb}	f_{Bb}	f_{Cc}	f_{Aa}	R_{240}	R_0	R_{120}
f_{Cc}	f_{Cc}	f_{Aa}	f_{Bb}	R_{120}	R_{240}	R_0

$D_n = \left\{ x^i y^i \,\middle|\, x^2 = e, y^n = e, xy = y^{-1}x; i = 0,1, j = 0,1, n-1 \right\}$

Is this an abelian group?

Solution:

(i) When $n=1$ is abelian if $n \geq 2$

$D_1 = \left\{ x^i y^j \,\middle|\, x^2 = e,\ y^1 = e, xy = y^{-1}x, i = 0,1, j = 0,1, n \right\}$

$y^{-1} = e$ then $xy = y^{-1}x$, $xe = e^{-1}x$, $xe = ex$, $xy = yx$; D_1 is abelian

(ii) When $n=2$, then

$y^2 = e \Rightarrow y \cdot y = e \Rightarrow y = y^{-1}$; From relation $xy = y^{-1}x = yx$; D_2 is an abelian group

(iii) When $n \geq 3$ then D_n is always non-abelian.

External Direct Product

Definition: Let $G_1, G_2, ...G_n$ be finite collection of groups. Then external direct product of $G_1, G_2, ...G_n$ is denoted by $G_1 \times G_2 \times ...... \times G_n$ or $G_1 \oplus G_2 \oplus ...... \oplus G_n$ and defined by

$$G_1 \times G_2 \times \ldots\ldots \times G_n = \{(g_1, g_2, \ldots. g_n) \mid g_i \in G_i, 1 \le i \le n\}$$
$$x = (g_1, g_2, \ldots. g_n) \in G_1 \times G_2 \times \ldots. \times G_n$$
$$y = (g_1^{'}, g_2^{'} \ldots. g_n^{'}) \in G_1 \times G_2 \times \ldots. \times G_n$$
$$xy = (g_1, g_2, \ldots. g_n) \cdot (g_1^{'}, g_2^{'}, \ldots g_n^{'})$$
$$= (g_1 g_1^{'}, g_2 g_2^{'}, \ldots. g_n g_n^{'})$$

Then each $g_i g_i^{'}$ performed with the operation of G_i.

<u>For example</u>:

$G_1 = Z_2$ and $G_2 = D_4$, then direct product of G_1 and G_2.

$$G_1 \times G_2 = Z_2 \times D_4 = \{(g_1, g_2) \mid g_1 \in Z_2, g_2 \in D_4\}$$

$$Z_2 \times D_4 = \begin{Bmatrix} (0, R_0), (0, R_{90}), (0, R_{180}), (0, R_{270}), (0, H), (0, V) \\ (0, D), (0, D'), (1, R_0), (1, R_{90}), (1, R_{180}), (1, R_{270}) \\ (1, H), (1, V), (1, D), (1, D') \end{Bmatrix}$$

$$x = (1, R_{270}) \in Z_2 \times D_4$$
$$y = (0, H) \in Z_2 \times D_4$$
$$x \cdot y = (1, R_{270})(0, H) = (1 + 0, R_{270} \cdot H)$$
$$= (1, D)$$

Note: Let $(g_1, g_2, \ldots. g_n) \in G_1 \times G_2 \times \ldots.. \times G_n$ then

$$O(g_1, g_2, \ldots. g_n) = \text{L.C.M.}(O(g_1) \text{ in } G_1, O(g_2) \text{ in } G_2 \ldots. O(g_n) \text{ in } G_n)$$

and $(g_1, g_2, \ldots g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots. g_n^{-1})$

Let's try to understand compositions between different elements and what does those imply.

Q. Translate each of the following multiplicative expressions into its additive counterpart.

(a) $a^2 b^3$ (b) $a^{-2}(b^{-1}c)^2$ (c) $(ab^2)^{-3} c^2 = e$

(a) $a^2 b^3 = (a \circ a) \cdot (b \circ b \circ b) = (a + a) + (b + b + b) = 2a + 3b$

(b) $a^{-2}(b^{-1}c)^2 = (a^{-1})^2 (b^{-1}c)^2 = (-a) + (-a) + (-b + c) + (-b + c) = -2a - 2b + 2c$

(c) $(ab^2)^{-3} c^2 = e$; $((a + b + b)^{-1}) + (c + c) = e$; $(-a - b - b)^3 + (c + c) = e$

$-3a - 6b + 2b + 2c = e$; $-3a - 6b + 2c = e$

Q. For any elements *a* and *b* from a group and any integer *n*, prove that
How to think!!

$\left(a^{-1}ba\right)^2=\left(a^{-1}ba\right)\cdot\left(a^{-1}ba\right)=a^{-1}b\left(a\circ a^{-1}\right)\left(ba\right)$ Associativity $=a^{-1}beba=a^{-1}b^2a$

$\left(a^{-1}ba\right)^3=\left(a^{-1}ba\right)^2\circ\left(a^{-1}ba\right)=\left(a^{-1}b^2a\right)\circ\left(a^{-1}ba\right)=a^{-1}b^2\left(a\circ a^{-1}\right)ba=a^{-1}b^2e\circ a=a^{-1}b^3a$

We are trying to use mathematical induction.

Let if it's true for $n=k$ i.e. $\left(a^{-1}ba\right)^k=a^{-1}b^ka$ then we need to show, its true for $n=k+1$ too.

$\therefore\ \left(a^{-1}ba\right)^{k+1}=\left(a^{-1}ba\right)^k\circ\left(a^{-1}ba\right)=\left(a^{-1}b^ka\right)\circ\left(a^{-1}ba\right)=a^{-1}b^k\left(a\circ a^{-1}\right)ba=a^{-1}b^{k+1}a$

Therefore its true for all $n\in\mathbf{N}$. Similarly we can show for negative integers.

Q. **(Law of exponents for Abelian group)**

Let a and b are any two elements of an Abelian group and let *n* be any integer. Show that $\left(ab\right)^n=a^nb^n$. Is this also true for non-Abelian groups?
Think!
Given, if G is an Abelian group. $\Rightarrow ab=ba$; $\forall a,b\in G$

$\because\ \left(ab\right)^2=\left(ab\right)\circ\left(ab\right)=\left(ab\right)\circ\left(ba\right)=ab^2a=aab^2=a^2b^2$

$\left(ab\right)^3=\left(ab\right)^2\circ\left(ab\right)=a^3b^3=\left(a^3a\right)\square\left(b^3b\right)$

Q. Prove that a group is abelian iff $\left(ab\right)^{-1}=a^{-1}b^{-1}$ for all a, b in G.

Think!

Let if G is abelian; then $ab=ba\Rightarrow\left(ab\right)^{-1}=\left(ba\right)^{-1}\Rightarrow b^{-1}a^{-1}=a^{-1}b^{-1}$

$\therefore\left(ab\right)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}$

Now if we have $\left(ab\right)^{-1}=a^{-1}b^{-1}$; then we want to check G is abeial?

For this; $\left(ab\right)\circ\left(ab\right)^{-1}=e$; we use $\Rightarrow\left(ab\right)\circ a^{-1}b^{-1}=e\Rightarrow aba^{-1}b^{-1}=e\Rightarrow aba^{-1}b^{-1}b=eb$

$\Rightarrow aba^{-1}=b\Rightarrow aba^{-1}a=ba\Rightarrow ab=ba\Rightarrow G$ is abelian.

Q. If $a_1,a_2,....,a_n$ belong to a graph, what is the inverse of $a_1,a_2,....,a_n$?

$\because\left(a_1a_2.....a_n\right)\cdot\left(a_n^{-1}a_{n-1}^{-1}a_{n-2}^{-1}....a_3^{-1}a_2^{-1}a_1^{-1}\right)$

$=a_1a_2......a_{n-1}a_n\cdot a_n^{-1}\cdot a_{n-1}^{-1}.....a_3^{-1}a_2^{-1}a_1^{-1}$

$=a_1a_2.....a_{n-1}\cdot a_{n-1}^{-1}......a_3^{-1}a_2^{-1}a_1^{-1}$

$=e$

$\therefore\quad\boxed{\left(a_1a_2.....a_n\right)^{-1}=a_n^{-1}a_{n-1}^{-1}a_{n-2}^{-1}.......a_3^{-1}a_2^{-1}a_1^{-1}}$

Q. Prove that every group table is a Latin Square.
(Such questions are to feel algebra expected in subjective exams like UPSC)
Latin Square: Each element of the group appears exactly one in each row and each column.
How to think!
Ans. Think by talking all axioms of a group into consideration.

Example: By closure axiom;
If $x \circ y = z$ then $x \circ y \neq z'$ where $z' \neq z$.

Q13. Let G be a finite group. Show that the number of elements x of G s.t. $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.
Think!!
$x^3 = e \Rightarrow$ either $x = e$ or $x^2 \neq e$
Because $x^2 = e$ and $x^3 = e$ possible only when $x = e$.
$x^2 \neq e \Rightarrow x$ is not self inverse element.

Q. In a finite group, show that the number of non-identity elements that satisfy the equation $x^5 = e$ is a multiple of 4.
Think!!
$x^4 = e$
(i) $x = e$ ($\because$ we need not identity $\therefore$ Not possible)
(ii) $x \neq e \Rightarrow G$ will have total no. of elements as either 5 or 10 or 15, ... (divisible by 5)

Q. Q_5^4 based on randomly (arbitrary) defined binary compositions. (Not standard examples). So for these, we need to just focus on basics.
Prob. (i)
Let $G = \mathbf{R}\{-1\}$ be the set of all real numbers omitting -1. Define the binary composition * on G by $A*B = a+b+ab$. Show that $(G,*)$ is a group. Is it abelian?
Closure: Let $x \in G \Rightarrow x \neq -1$; $y \in G \Rightarrow y \neq -1$
Now we need to show $x*y = -1 \Rightarrow x+y+xy \neq -1$
If can be noticed that $x+y+xy = -1$ is possible only when $x=-1, y=-1$
[Observe $x<0, y<0$; then $(x+y)$ and xy will have opposite signs]
Associative: Real numbers follow associativity
$\therefore (a*b)*c = a*(b*c)$
Identity: Let $\exists\ e \in G$ s.t. $a*e = a \Rightarrow a+e+ae = a \Rightarrow e(1+a) = 0 \Rightarrow e = 0 \neq -1 \therefore e \in G$
Inverse: For each $a \in G$, $e = 0 \in G$, Let if there exists $b \in G$ s.t. $a*b = e$
$\Rightarrow a+b+ab = 0 \Rightarrow b(1+a) = -a \Rightarrow b = \dfrac{-a}{1+a} \neq -1 \therefore b \in G$
So inverse axiom also satisfied.
For abelian:
$a*b = a+b+ab$
$= b+a+ba$ $\because$ a and b are reals, $\therefore$ commute
Therefore $(G,*)$ is an abelian group.

Q. On $\mathbf{R}^3$, define a binary operation * as follows: For $(x,y,t),(x',y',t')$ in $\mathbf{R}^3$,
$$(x,y,t)*(x',y't') = \left(x+x', y+y', t+t' + \frac{1}{2}(x'y - xy')\right)$$
Then show that $(\mathbf{R}^3,*)$ is a group.

NOTE: At the first sight it may look like absurd. But if you think about $\mathbf{R}^3$; component wise addition, you'll feel, its actually easy.

$\Rightarrow$Addition, subtraction and multiplication of real numbers is again a real number because $\left(\mathbf{R}^3,*\right)$ is closed.

Associative:

Let $(x,y,t)\in\mathbf{R}^3,(x'y't')\in\mathbf{R}^3,(x'',y'',t'')\in\mathbf{R}^3$

then

$$(x,y,t)*\left[(x',y',t')*(x'',y'',t'')\right]$$

$$=(x,y,z)*\left[x'+x'',y'+y'',t'+t''+\frac{1}{2}(x''y'-x'y'')\right]$$

$$=\left\{x+x'+x'',y+y'+y'',t+t'+t''+\frac{1}{2}(x''y'-x'y'')+\frac{1}{2}\{(x'+x'')y-y''(x+x')\right\}$$

$\therefore\left(\mathbf{R}^3,*\right)$ is associative.

Identity: It can be observed easily that $(0,0,0)\in\mathbf{R}^3$ is an identity element here.

Inverse: After observing identity; its easy to observe

$$(x,y,t)^{-1}=(-x,-y,-t)$$

$\therefore\left(\mathbf{R}^3,*\right)$ is a group.

Q. Write elements of $S_3\times\mathbf{Z}_3$ and then find composition of two different elements of it.

$\because S_3=\{I,\sigma_1,\sigma_2,\sigma_3,T_1,T_2\}$, $\mathbf{Z}_3=\{0,1,2\}$

$$\therefore S_3\times\mathbf{Z}_3=\begin{Bmatrix}(I,0),(I,1),(I,2),(\sigma_1,0),(\sigma_1,1),(\sigma_1,2),(\sigma_2,0),(\sigma_2,1)(\sigma_2,2)\\(\sigma_3,0),(\sigma_3,1),(\sigma_3,2),(\tau_1,0),(\tau_1,1),(\tau_1,2),(\tau_2,0),(\tau_2,1),(\tau_2,2)\end{Bmatrix}$$

$$(\sigma_2,1)*(\tau_2,2)=(\sigma_2\cdot\tau_2,1+_3 2)=(\sigma_1,0)$$

$$\because\sigma_2\circ\tau_2=(13)(123)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)=\tau_1$$

Q. Find α^3, where $\alpha=(\sigma_2,j,2)\in S_3\times Q_8\times\mathbf{Z}_5$

$$\because\ \alpha^3=\alpha*\alpha*\alpha=(\sigma_2,j,2)\times(\sigma_2,j,2)\times(\sigma_2,j,2)$$

$$=\left(\sigma_2\circ\sigma_2\circ\sigma_2,j\cdot j\cdot j,2+5^2+5^2\right)=\left(\sigma_2^3,j^3,6\,\text{in}\,\mathbf{Z}_5\right)=\left(\sigma_2^2\circ\sigma_2,j^2\cdot j,1\right)=\left(I\circ\sigma_2,-1\cdot j,1\right)$$

$$=(\sigma_2,-j,1)$$

open problem (based on Dihedral Group)

Q. Let f and g be the functions from $\mathbf{R}/\{0,1\}$ to $\mathbf{R}$ defined by $f(x)=1/x$ and $g(x)=\dfrac{x-1}{x}$ for $x\in\mathbf{R}/\{0,1\}$. Can you try to construct a smallest group of functions with the above functions which is isomorphic to S_3 or D_3?

Observation: $(f\circ g)(x)=f(g(x))$

$$=f\left(\frac{x-1}{x}\right)=\frac{1/x\,(x-1)/x}{x-1}$$

$$(g \circ f)(x) = g(f(x))$$

$$= g\left(1/x\right) = \frac{1/x - 1}{1/x}$$

$$\boxed{g \circ f = f \circ g^{-1}}$$

$$(g \circ f)(x) = f \circ g^{-1} = f \circ g^{2} = f\left(\frac{-1}{x-1}\right) = 1 - x$$

Assignment # 2

Subgroups, Centre of a group, Order of element of a group, cyclic groups, homomorphism, Isomorphism basic definitions

Homomorphism

Let $(G_1, 0)$ and $(G_2, *)$ are two groups A mapping $f:(G_1, 0) \to (G_2, *)$ is homomorphism if

$f(x \circ y) = f(x) * f(y);\ x, y \in G_1,\ f(x), f(y) \in G_2$

e.g.

Q. $f: Z_4 \to Z_{10}$ defined by $f(x) = 0 \cdot x$ is homomorphism?

Solution:

$f: Z_4 \to Z_{10}$

$f(x) = 0 \cdot x$

$f(x+y) = 0 \cdot (x+y) = 0 \cdot x + 0 \cdot y$

$= f(x) + f(y),\ \forall x, y \in Z_4$

Yes.

Isomorphism

A mapping $f: G \to G'$ is said to be isomorphism if

(i) *f* is homomorphism
(ii) *f* is one-one
(iii) *f* is onto

Q. $f: Z \to Z,\ f(x) = 1 \cdot x$ is isomorphism?

Solution:

f is homomorphism, one-one and onto then *f* is isomorphism.

Similarly

$f: Z \to Z = -x$ is also, homomorphism, one-one and onto then $f(x) = -x$ is isomorphism.

Q. $f: Z_{15} \to Z_{15},\ f(x) = 1 \cdot x$ is isomorphism?

Solution:

$f(x) = 1 \cdot x,\ O(1)$ in $Z_{15} = 15,\ Z_{15}$ (LHS)

has element of order 15 then $f(x) = 1 \cdot x$ is homomorphism.

***f* is one-one**:

$f(x_1) = f(x_2),\quad x_1, x_2 \in Z_{15}$ (LHS)

$\Rightarrow x_1 = x_2$

f is one-one.

***f* is onto**: $O(Z_{15}(\text{LHS})) = O(Z_{15}(\text{RHS})) = 15$ and *f* is one-one then *f* is onto.

Q. $f: Z_{20} \to Z_{20}$, how many isomorphism?

Solution:

20|20, then no. of onto homomorphism

$= \phi(20) = 8$ = one-one homomorphism

(cardinality of domain and co-domain are same).
and they are:

$$\left.\begin{array}{l} f(x)=1\cdot x \\ f(x)=3\cdot x \\ f(x)=7\cdot x \\ f(x)=9\cdot x \\ f(x)=11\cdot x \\ f(x)=13\cdot x \\ f(x)=17\cdot x \\ f(x)=19\cdot x \end{array}\right\} \text{isomorphism in } f: Z_{20} \to Z_{20}$$

Properties of Isomorphism

Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then

(i) ϕ carries the identity of G to the identity of $\bar{G}$

(ii) For every integer *n* and for every group element *a* in G, $\phi(a^n) = [\phi(a)]^n$

(iii) For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.

(iv) G is abelian if and only if $\bar{G}$ is abelian.

(v) $|a| = |\phi(a)|$ for all a in G. (Isomorphism preserves orders)

(vi) G is cyclic if and only if $\bar{G}$ is cyclic.

(vii) For a fixed integer *k* and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\bar{G}$.

(viii) ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.

(ix) If *k* is a subgroup of G, then $\phi(k) = \{\phi(k) : k \in K\}$ is a subgroup of $\bar{G}$.

Q1. Let G be an Abelian group under multiplication w.r.t multiplication with identity *e*. Let $H = \{x^2 | x \in G\}$. Then H is a subgroup of G?

$\because\ e^2 = e \ \therefore e^2 \in H \ \therefore H$ is non-empty.

Let $x^2 \in H, y^2 \in H$

$\Rightarrow x^2 \cdot y^2 = (xy)^2$

$\Rightarrow x^2 y^2 \in H$

$\because$ Given Group is abelian

$\therefore\ (xy)^m = x^m y^m$

Also we can show $x^2 (y^2)^{-1} \in H$

$\because$ for abelian group $(y^2)^{-1} = (y^{-1})^2 = z^2$ where $z = y^{-1}$

$\therefore$ By one step subgroup test H is a subgroup of G.

Q2. Let G be the group of non-zero real numbers under multiplication. $H = \{x \in G \mid x = 1 \text{ or irrational}\}$ and $K = \{x \in G \mid x \geq 1\}$. Then $H \leq G$? $k \leq G$?

H is not a subgroup of G.

$\because \sqrt{2} \in H, \sqrt{2} \in H$

But $\sqrt{2} \times \sqrt{2} = 2 \notin H$

K is not a subgroup of G $\because$ for $2 \in K, 2^{-1} = \frac{1}{2} \notin k$

Q3. Let G be a group, and let a be any element of G. Then $\langle a \rangle$ is a subgroup of G.

$H = \langle a \rangle$ represents a set with elements as integral powers of a (that is composition of a with itself as integral times)

$\because a \in H \ \therefore$ H is non-empty

Let $x = a^n \in H$, $y = a^m \in H$

then $a^n \left(a^m\right)^{-1} = a^{n-m} \in H$

$\therefore H$ is a subgroup of G.

Q4. In $\mathbf{Z}_{10}$, where $H = \langle 2 \rangle$

We know that in $\mathbf{Z}_n$; a^n means na.

$\therefore H = \langle 2 \rangle = \{2, 4, 6, 8, 0\}$

Q5. In $U(10)$, write $H = \langle 3 \rangle$.

$H = \{3, 3^2, 3^3, 3^4\} = \{3, 9, 7, 1\} = U(10)$

Q6. Let $G = GL_2(\mathbf{R})$. Let $H = \{a \in G \,\|A| \text{ is a power of } 2\}$. Show that H is a subgroup of G.

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, |I| = 1 = 2^\circ \quad \therefore I \in H \quad \therefore$ H is non-empty.

Let $A \in H$, $B \in H$

$\Rightarrow |A| = 2^n, \Rightarrow |B| = 2^m$

$\therefore |AB| = |A| \cdot |B| = 2^n \cdot 2^m = 2^{n+m}$

Also, we can think $\left|AB^{-1}\right| = |A|\left|B^{-1}\right| = |A| \cdot \frac{1}{|B|} = 2^n \cdot 2^{-m} = 2^{n-m}$

$\Rightarrow AB^{-1} \in H$

$\therefore H$ is a subgroup of G.

Q7. Let $G = GL_2(\mathbf{R})$ and $H \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \, a \text{ and } b \text{ non-zero integers} \right\}$. Prove or disprove that H is a subgroup of G.

$\because I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H \ \therefore H$ is non-empty

Let $A \in H$ where $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, |A| = ab$

$B \in H$ where $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}, |B| = cd$

$$AB^{-1} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} 1/c & 0 \\ 0 & 1/d \end{bmatrix} = \begin{bmatrix} a/c & 0 \\ 0 & b/d \end{bmatrix} \in H$$

$\therefore H \le G$

Q8. Let G be a group of functions from $\mathbf{R}$ to $\mathbf{R}^*$ under multiplication. Let $H = \{ f \in G \text{ such that } f(1) = 1 \}$. Prove that H is a subgroup of G.

Let $f \in H,\ g \in H$

$\Rightarrow f(1) = 1 \Rightarrow g(1) = 1$

$\therefore\ f \cdot g(1) \Rightarrow f(g(1)) = f(1) = 1$

$\Rightarrow f \cdot g \in H$

Also we can show that that $fg^{-1}(1)$

$= f(g^{-1}(1))$

$= f(1) = 1$

$= 1$

$\Rightarrow fg^{-1} \in H$

$$\text{H is non-empty} \Rightarrow \begin{cases} \because \exists \phi \in H \ s.t. \\ f \cdot \phi = f \\ \because\ f\phi(1) = f(1) \\ f(\phi(1)) = 1 \\ \Rightarrow \phi(1) = f^{-1}(1) \\ \Rightarrow \phi(1) = 1 \end{cases}$$

$\because \phi$ is identity element of H.

Order of Element: Order of element *a* in G is the least positive integer *n* s.t. $a^n = e$. IF such type of *n* does not exist then the order of *a* is infinite.

Q. Possible order of elements in Z
Solution:
$Z = \{0, +1, +2, +3, ...\}$
$1 \cdot 0 = 0$ then $O(0) = 1$
$1 \in Z$ s.t. $O(1) = \infty$
If $0 \neq a \in Z$ then, $O(a) = \infty$
Then possible order of elements in Z is 1 and ∞ .

Q. How many elements of order finite in Z?
Solution: Exactly one element of order finite in Z i.e. 0
Q. Possible order of elements in $\mathbf{Q}, \mathbf{R}, \mathbf{C}$?
Solution: Same as Z, 1 and ∞
Q. Possible order of elements in Q.
Solution:
Q* is group under multiplication then $a \in Q^*$ and $O(0) = 1$, $a^n = 1$, where *n* is least positive integer.
$1 \in Q^*$ s.t. $1^1 = 1$ then $O(1) = 1$
$-1 \in Q^*$ s.t. $(-1)^2 = 1$ then $O(-1) = 2$
$2 \in Q^*$ s.t. $O(2) = \infty$
Q. How many element of order finite in Q^* ?
Ans. Two elements of order finite in Q^* say 1 and -1.
Possible order are 1, 2, ∞
Q. Possible order of elements in R^* ?
Ans. 1, 2, ∞ (Possible orders)
Q. Possible orders of elements in C^* ?
Infinite number of elements in $\mathbf{C}^*$

Q. What are the possible order of elements in Q_4
Ans. $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$
$a^n = e$ identity = 1
$1 \in Q^4 \Rightarrow O(1) = 1$
$-1 \in Q^4 \Rightarrow O(-1) = 2$
$i \in Q_4 \Rightarrow O(i) = 4$
$-i \in Q_4 \Rightarrow O(-i) = 4$
$j \in Q_4 \Rightarrow O(j) = 4$

$-j \in Q_4 \Rightarrow O(-j) = 4$

$k \in Q_4 \Rightarrow\Rightarrow O(k) = 4$

$-k \in Q_4 \Rightarrow\Rightarrow O(-k) = 4$

$j^2 = -1, \Rightarrow j^2 \cdot j^2 = j^4 = 1$

Possible order of elements in Q_4 is 1,2 & 4

Number of elements of order 1 in $Q_4 = 1$

Number of elements of order 2 in $Q_4 = 1$

Number of elements of order 4 in $Q_4 = 6$

Q. Find possible order of element in Z_{10} ?

Ans. $Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$

$O(0)=1, O(1)=10, O(2)=5, O(3)=10\ O(4)=5, O(5)=2, O(6)=5, O(7)=10, O(8)=5, O(9)=10$ Explanation: 1+1+1+1+1+1+1+1+1+1 = 0 $O(1)=10$ Additive identity = 0 Every identity element is of the order is 1 $O(0)=1$

Possible orders of elements 1, 2, 5, and 10

Number of elements with order 1 in $Z_{10} = 1$

Number of elements with order 2 in $Z_{10} = 1$

Number of elements with order 5 in $Z_{10} = 4$

Number of elements with order 10 in $Z_{10} = 4$

Q. Possible order of elements in K_4 ?

Ans. Possible orders are 1 and 2

Q. Find elements of possible order in $U(8)$.

$O(U(8)) = 4, O(1) = 1, O(3) = 2, O(5) = 2$; since $3 \cdot 3 = 3^2 = 9 = 1(\text{mod}\,8)$, $O(7) = 2$

Possible order of elements in $U(8) = 1$ and 2.

Number of elements of order 1 in $U(8) = 1$ and Number of elements of order 2 in $U(8) = 3$

Q. Find possible order of elements in $U(15)$.

Ans.

$U(15) = \{1,2,4,7,8,11,13,14\}$

$O(U(15)) = 8$

$O(1) = 1$ $\quad$ $O(14) = 2$

$O(2) = 4$

$O(4) = 2$

$O(7) = 4$

$O(8) = 4$

$O(11) = 2$

$O(13) = 4$

Possible order of elements in $U(15) are 1, 2, 4$

Number of elements of order 1 = 1
Number of elements of order 2 = 2
Number of elements of order 4 = 4

Exam Point
In D_n

1- No. of elements of order 2 in D_n

$$= \begin{cases} n+1, \text{ if } n \text{ is even} \\ n, \text{ if } n \text{ is odd} \end{cases}$$

2. Number of elements of order d other than 2; If $2 \neq d/n$ then the no. of elements of order *d* in $D_n = \phi(d)$

Q. Find possible order of elements in D_1.

Ans. $D_1 = \{R_0, f_0\}$, $O(D_1) = 2\times 1 = 2$; $O(R_0) = 1$, $O(f_0) = 2$

Possible orders of elements 1 and 2

Number of elements of order 1 in $D_1 = 1$ and Number of elements of order 2 in $D_1 = 1$.

Q. Find possible order of elements in D_3?

No. of Rotations = No. of Reflections

$O(R_0) = 1, O(R_{120}) = 3, O(R_{240}) = 3, O(f_{Aa}) = 2, O(f_{Bb}) = 2, O(f_{Cc}) = 2$

Possible order of elements in D_3 1 and 3

Number of elements with order 1 = 1
Number of elements with order 2 = 3
Number of elements with order 3 = 2

Q. Find possible order of elements in D_4.

Since possible Order of elements are 1, 2 & 4

Identity element $R_0 \in D_4$ such that $O(R_0) = 1$

$O(R_{90}) = 4$

$O(R_{180}) = 2 \quad O(R_{270}) = 4$

$O(H) = 2, O(V) = 2, O(D) = 2, O(D') = 2$

Number of elements of order 1 in $D_4 = 1$

Number of elements of order 2 in $D_4 = 5$

Number of elements of order 4 in $D_4 = 2$

Q. Find possible order of elements in D_{10}?

Ans. Possible orders of elements in D_{10} are 1, 2, 5, 10

Number of elements of order 1 = $\phi(1) = 1$

Number of elements of order 2 in D_{10} (since n is even so) $= 10 + 1 = 11$

Number of elements of order 5 in $D_{10} = \phi(5) = 4$

Number of elements of order 10 in $D_{10} = \phi(10) = 4$

Exam Point. If $O(a) = n \Rightarrow a^n = e$ but $a^n = e$ does not implies that $O(a) = n$.

Proof: If $a^n = e \Rightarrow O(a) | n$; $a \in G$

Let $O(a) = K$. $a^n = 0$ ….(1)

$O(a) = K$ ….(2)

Then by division algorithm, ; $n = k_q + r$ ….(3);

$0 \le r < k$

Case I: If $r = 0$ then $n = k_q \Rightarrow k | n \Rightarrow O(a) | n$

Case II: $r \ne 0$

$e = a^n = a^{kq+r} \Rightarrow e = a^n = a^{kq} a^r = (a^k)^q \cdot a^r = e^q \cdot a^r \Rightarrow e = a^r$. $O(a) = r$ where $r < k$

Which contradicts the fact that $O(a) = K$. Hence *r* must be equal to O $\therefore$ $O(a) | n$

From (3)

$n = k_{q+r}$

$n = k_{q+0} \Rightarrow n = k_q \Rightarrow k | n \Rightarrow O(a) | n$

Exam Point. Show that $O(a) = O(xax^{-1}) = O(x^{-1}ax)$ $x, a \in G$

Let G be a group and $O(a) = n \Rightarrow a^n = e$ ….(1

$(xax^{-1})^2 = (xax^{-1})(xax^{-1}) = xax^{-1}xax^{-1} = xaeax^{-1} = xa^2x^{-1}$

$(xax^{-1})^3 = (xax^{-1})^2(xax^{-1}) = (xa^2x^{-1})(xax^{-1}) = xa^2x^{-1}xax^{-1} = xa^2eax^{-1} = xa^3x^{-1}$

Similarly

$(xax^{-1})^n = xa^nx^{-1} = xex^{-1}$ From $(1) = e$

Since n is least positive integer then

$O(xax^{-1}) = n = O(a)$

$O(a) = 0(xax^{-1})$ and similarly; $O(a) = O(x^{-1}ax)$

Hence $O(a) = O(xax^{-1}) = O(x^{-1}ax)$

Exam Point. Show that $O(ab) = O(ba),\ \forall a,b \in G$

Proof: $ab = abe = abaa^{-1} = a(ba)a^{-1}$ $O(x(ba)x^{-1} = O(ba))$. So $O(ab) = 0(a(ba)a^{-1})$

$\because O(ab) = 0(ba)$ $(O(xax^{-1}) = O(a))$

Exam Point. Show that $(ab)^{-1} = b^{-1}a^{-1}, a,b \in G$

Proof: $abb^{-1}a^{-1} = e$ $\because aa^{-1} = e$

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

$$\boxed{(ab)^{-1} = b^{-1}a^{-1}}$$

Exam Point. Show that $O(a) = O(a^{-1})$

Proof: Let $O(a) = n \Rightarrow a^n = e$

Taking Inverse both sides $\Rightarrow (a^n)^{-1} = e^{-1} \Rightarrow a^{-n} = e \Rightarrow (a^{-1})^n = e \Rightarrow O(a^{-1}) = n = O(a)$

$\therefore\ O(a) = O(a^{-1})$

Theorem: If every element of G has self inverse then G is abelian but converse need not be true.
Proof: Let G be a group and every element of G has self inverse

$a \in G \Rightarrow a^{-1} = a$ ….(1

$b \in G \Rightarrow b^{-1} = b$ ….(2)

Also $a \in G, b \in G \Rightarrow ab \in G \Rightarrow (ab)^{-1} \in G \Rightarrow b^{-1}a^{-1} = ab \Rightarrow ba = ab\ \forall\ a,b \in G$

Note- if $a^2 = e$ $\forall$ a, elements of group G then G will be abelian but its converse need not be true.
i.e. $ab = ba$
$\Rightarrow G$ is an abelian group
Converse, need not be true

$Z_4 = \{0,1,2,3\};\ 0^{-1} = 0, 1^{-1} = 3, 2^{-1} = 2, 3^{-1} = 1$

Only 0 and 2 are self inverse . But Z_4 is abelian group.

Cyclic Group: A group G is said to be cyclic group if $\exists$ element 'a' in G s.t. every elements of G generated by 'a' i.e. $G=\left\{a^n \middle| n\in \mathbf{Z}\right\}$. Also represented as $G=\langle a\rangle$

Example- $Z_6=\{0,1,2,3,4,5\}$ is Cyclic Group?

Solution: YES. Reason: $1\in Z_6$ s.t.

$1=1, 1+1=2, 1+1+1=3, 1+1+1+1=4, 1+1+1+1+1=5, 1+1+1+1+1+1=6=0$

Then 1 is generator of Z_6 i.e. $G=\langle 1\rangle$ i.e. $Z_6=\langle 1\rangle$

$5=5, 5+5=4, 5+5+5=3, 5+5+5+5=2, 5+5+5+5+5=1, 5+5+5+5+5+5=30=0$

Then 5 is also a generator of Z_6 i.e. $G=\langle 5\rangle$ i.e. $Z_6=\langle 5\rangle$

Thus, Z_6 is a Cyclic Group.

Exam Point. If G is Cyclic then G is abelian

Proof: If G is cyclic then G is abelian

Let G is Cyclic group then $\exists\ a\in G$. $G=\langle a\rangle$

Suppose $x\in G$ then $x=a^n, n\in \mathbf{Z}$ and $y\in G$ then $y=a^n$, $m\in \mathbf{Z}$

$x\cdot y=a^n\cdot a^m=a^{n+m}=a^{m+n}=a^m a^n$ ($n+m=m+n$ because Z is abelian)$=y\cdot x$

$\therefore xy=y\cdot x$, $\forall x,y\in G$. Hence, G is abelian.

Converse, of above statement need not be true i.e. If G is abelian then G need not be Cyclic

$K_4=\left\{e,a,b,ab \middle| a^2=e, b^2=e, ab=ba\right\}$

Let us consider

$a^1=a$, $b^1=b$; $(ab)^1=ab$. $\quad a^2=e$, $b^2=e$; $(ab)^2=e$

$a^3=a$ $b^3=b$ $(ab)^3=ab$, $a^4=e$ $\quad b^4=e$

A generate only 2 elements of K_4 say *a* & *e* thus a is not generator of K_4.

Q. Show that Z is Cyclic group w.r.t usual addition

Solution:

$Z=\{0,\pm1,\pm2,...\}$, $a=1\in \mathbf{Z}$ s.t. $G=\langle 1\rangle=\left\{na \middle| n\in Z\right\}=\left\{n1 \middle| n\in Z\right\}$

since 1 in generator of Z so $G=Z$ is cyclic.

Now, $-1\in Z$ s.t $G=Z=\langle -1\rangle=\left\{n(-1) \middle| n\in Z\right\}$. Thus -1 is also generator of $\mathbf{Z}$.

Therefore 1 and -1 are generator of $\mathbf{Z}$ i.e. exactly two.

Q. $(\mathbf{Q}^+)$ is cyclic?, $(\mathbf{R}^+)$ is cyclic?, $(\mathbf{C}^+)$ is cyclic?, $(\mathbf{Q}^*)$ is cyclic?, $(\mathbf{R}^*)$ is cyclic?, $(\mathbf{C}^*)$ is cyclic?

Which of the above are cyclic group?

Ans. None of them are cyclic

Hint: $a\notin Q$ s.t $Q=\langle a\rangle=\left\{na \middle| n\in \mathbf{Z}\right\}$.

Q. Is $U(12)=\{1,5,7,11\}$ cyclic?

Ans.
$1 \in U(12)$ s.t $O(1)=1, 5 \in U(12)$ s.t $O(5)=2$
$7 \in U(12)$ s.t $O(7)=2, 11 \in U(12)$ s.t $O(11)=2$
$O(U(12))=4$ and $U(12)$ has no element of order 4 then $U(12)$ is not cyclic.

Q. Is D_1 a cyclic group?
Ans. $O(D_1)=2 \cdot 1=2$ and D_1 has element of order 2 then D_1 is a cyclic group.
Q. Is D_2 a cyclic group?
Ans. $O(D_2)=4$ and D_2 has no element of order 4 then D_2 is not cyclic.
Q. Is D_n, $n \geq 3$ cyclic?
Ans. $D_n, n \geq 3$ is non-abelian then D_n is non-cyclic.

Q. $GL_n(\mathbf{F})_{n>1}$ is cyclic?
Ans. $GL_n(\mathbf{F}) = \left\{ A = \left[a_{ij} \right]_{n \times n} \middle| a_{ij} \in \mathbf{F}, \text{and} |A| \neq 0 \right\}$
$(GL_n(\mathbf{F}))$ is non-abelian (because matrix multiplication need not be commutative) then $GL_n(\mathbf{F})$ is not cyclic.

- If $n=1$ then $GL_1(\mathbf{R})$ is it cyclic?

Solution: If $n=1$ then $GL_1(\mathbf{R})=R^*$ and $\mathbf{R}^*$ is abelian but not cyclic hence $GL_1(\mathbf{R})$ is abelian but not cyclic.

Q.(i) $SL_n(\mathbf{F})$, $n>1$ is cyclic? ii) If $n=1$ then $SL_n(\mathbf{F})$ is cyclic?
Ans.(i) $SL_n(\mathbf{F})$ is non-abelian if $n \geq 2$ then $SL_n(\mathbf{F})$ is not cyclic.
(ii) If $n=1$ then $SL_n(\mathbf{F}) = \left\{ A = \left[a_{ij} \right] \middle| |A|=1, a_{ij} \in \mathbf{F} \right\} = \{1\}$
$O(SL_1(\mathbf{F}))=1$ and $SL_1(\mathbf{F})$ has a element of order 1 then $SL_1(\mathbf{F})$ is cyclic.

Q. $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$ is cyclic?
Solution: $i \in Q_4$ and $ij = -ji \neq ji$ $j \in Q_4$ and $ij \neq ji$ then Q_4 is non-abelian thus Q_4 is non-cyclic.

Q. Show that Z_n is cyclic?
Ans. Proof: Case I:
If $n=1, Z_1=\{0\}$ And $O(Z_1)=1$, $O \in Z_1$ s.t $O(0)=1 \Rightarrow Z_1$ has element of order 1 then Z_1 is cyclic.
Case II: If $n \geq 2$ then
$1 \in Z_n$ s.t $O(1)=O(Zn)$. Thus Z_n is cyclic.
Exam Point. No. of Generators in $Z_n = \phi(n)$: generator of Z_n; which is relatively prime to n i.e. $\gcd(a,n)=1$

- If $a \in Z_n$ s.t $\gcd(a,n)=1$ then a will be generator of Z_n.

Q. How many generators in Z_{20}?

Solution: $Z_{20} = \{0,1,2,3,...,19\}$. Number of generators in $Z_{20} = \phi(20) = 8$

These generators are $1,3,7,9,11,13,17$ & 19.

Q. $G = \{5,15,25,35\}$ is group under multiplication modulo 40? If yes then what is relation with $U(8)$?

Solution:

$G = \{5,15,25,35\}$. Consider composition Table w.r.t modulo 40

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

(i) Closure property $\forall a,b \in G \Rightarrow ab \in G$ (ii) Associative $a\cdot(bc) = (ab)\cdot c, \ \forall \ a,b,c \in G$

(iii) Identity $\forall \ \ a \in G \Rightarrow 25 \in G$ s.t $a\cdot 25 = 25\cdot a = a$

(iv) Inverse of each element of G

$5^{-1} = 5, 15^{-1} = 15, 25^{-1} = 25, 35^{-1} = 35$

Then $G = \{5,15,25,35\}$ is group w.r.t multiplication modulo 40

Every element in G has its self inverse hence G is abelian.

G is not cyclic because $O(G) = 4$ and it does not have any element of order 4 in it.

Note: G has only one element of order 1 and three elements of order 2.

- $U(8) = \{1,3,5,7\}$ also consider comparison table w.r.t multiplication modulo 8

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Every element of $U(8)$ has self inverse $1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$. $U(8)$ is a abelian group of order 4.Now, $U(8)$ is not cyclic because $U(8)$ has no element of order 4.

$U(8)$ has only one element of order 1 & 3 element of order 2 hence.

$G \approx U(8)$ i.e. G is isomorphic to $U(8)$.

Exam Point.

$Z_m \times Z_n$

If we have to find no. of elements of order k then first of all check that k^{th} order element exist or not by choosing d_1 & d_2 such that L.C.M. $(d_1, d_2) = K$, and $d_1 | m$ and $d_2 | n$ and number of elements of order K in $Z_m \times Z_n$

$= \sum(\phi(d_1) \times \phi(d_2))$ s.t $d_1 | m$ and $d_2 | n$

Q. $Z_2 \times Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

Clearly, $(0,1)(1,0) = (1,1) \in Z_2 \times Z_2$

$(1,1)(1,1) = (2,2) = (0,0) \in Z_2 \times Z_2$

$(0,1)(0,1) = (0,2) = (0,0) \in Z_2 \times Z_2$

$(1,0)(0,0) = (1,0) \in Z_2 \times Z_2$

$Z_2 \times Z_2$ is not a cyclic group but abelian.

$Z_2 = \{0,1\}$, $Z_3 = \{0,1,2\}$

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

$(1,1) \in Z_2 \times Z_3$; $(1,1) = (1,1)$; $(1,1)(1,1) = (2,2) = (0,2)$; $(1,1)(1,1)(1,1) = (3,3) = (1,0)$

$(1,1)(1,1)(1,1)(1,1) = (4,4) = (0,1)$; $(1,1)(1,1)(1,1)(1,1)(1,1) = (5,5) = (1,2)$

$(1,1)(1,1)(1,1)(1,1)(1,1)(1,1) = (6,6) = (0,0)$. Therefore $O(1,1) = 6$

Hence $Z_2 \times Z_3$ is a cyclic group as $O(1,1) = O(Z_2 \times Z_3)$ = 6.

Q. Find possible order of elements in $Z_2 \times Z_2$?

Solution: $G = Z_2 \times Z_2$. We need L.C.M. $(d_1, d_2) = K$ dividing 4

L.C.M. $(d_1, d_2) = 1$ is possible in $Z_2 \times Z_2$ as $d_1 | 2,\ d_2 | 2$

If $d_1 = 1,\ d_2 = 1$ then $\phi(1)\phi(1) = 1$. So Number of elements of order 1 is only 1

Now, L.C.M. $(d_1, d_2) = 2$ also possible in $Z_2 \times Z_2$

$d_1 | 2, d_2 | 2$, L.C.M. $(2,1) = 2$. means number elements of order 2 in Z_2 and elements of order1 in Z_2 which are $\phi(2)\phi(1) = 1$. Similarly let's check other possibilities:

$d_1 | 2, d_2 | 2$, L.C.M. $(1,2) = 2$. $\phi(1)\phi(2) = 1$

$d_1 | 2, d_2 | 2$ L.C.M. $(2,2) = 2$. $\phi(2)\phi(2) = 1$

No. of elements of order 2 are 3. Total = 3 elements.

Q. Find Number of elements of all possible orders in $Z_2 \times Z_4$.

L.C.M. $(d_1, d_2) = 1$, L.C.M. $(1,1) = 1$ $\phi(1)\phi(1) = 1$

Then only one element of order 1

Number of elements of order 2 in $Z_2 \times Z_4$ is 3 L.C.M. $(d_1, d_2) = 2$

$Z_2 \times Z_4$			
1	2	$\phi(1)\phi(2) = 1$	
2	1	$\phi(2)\phi(1) = 1$	Total 3 elements having order 2
2	2	$\phi(2)\phi(2) = 1$	

Then L.C.M. $(d_1, d_2) = 4$

$Z_2 \times Z_4$			
1	4	$\phi(1)\phi(4) = 1 \times 2 = 2$	Total = 4 elements having order 4
2	4	$\phi(2)\phi(4) = 1 \times 2 = 2$	

Possible orders are 1, 2 & 4 & respectively the number of elements of these orders are 1, 3 and 4.

COSET THEORY

Coset- Let H b e a subgroup of G and $a \in G$ then $a.H = \{ah | h \in H\}$ is called left coset of H in G and $Ha = \{ha | h \in H\}$ is called right co set of H in G.

Note: If G is abelian then left coset of H in G is equal to right coset of H in G.
Let aH is left coset of H in G then
$aH = \{ah | h \in H \text{ and } a \in G\} = \{ha | h \in H \text{ and } a \in G\} = Ha$ $\boxed{aH = Ha}$

Point- **H be a subgroup of G then show that** $HH = H$
Let G be a group and H be a subgroup of G then
$HH = \{h_1h_2 | h_1 \in H, h_2 \in H\}$
Let $x \in HH \Rightarrow x \in h_1h_2 \in H.Hh_1 \in H, h_2 \in H \Rightarrow h_1 \in H, h_2 \in H \Rightarrow h_1h_2 \in H \Rightarrow x = h_1h_2 \in H$
$x \in H$; $HH \subset H$
Let $h \in H \Rightarrow h = he \in HH$, $h \in H, e \in H \Rightarrow h \in HH \Rightarrow H \subseteq HH$
From (1) and (2) $H = HH$
e.g. $H = \{e, a, b\}$; $HH = \{ee, ea, eb, ab\} = \{e, a, b\}$ $ab \in H$ due to closure property = H

Point- **If** $a \in H$ **then** $aH = H$ **. Prove**
Let $ah \in aH$, $a \in H, h \in H$ $a \in H, h \in H \Rightarrow ah \in H$ …(1)
$a^{-1}h = h_1 \in H$. $h = ah_1 \in aH$; $H \subseteq aH$ ….(2)
From (1) and (2) $aH = H$

Q. Let G be a finite cyclic group of order G with generated by a and H be a subgroup of G generated by a^2 then find Right coset and left coset of H in G.
Hint:
G is a group generated by a, $G = \langle a \rangle \Rightarrow G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$
And H is a subgroup of G generated by a^2 Then $H = \{a^2, a^4, a^6 = e\}$

Exam Point- No. of cosets of subgroup H in G $= \dfrac{O(G)}{O(H)}$

Example-. $G = Q_4, H = \{1, -1\}$. Finding cosets of H in G
$1 \in Q_4$ s.t $1H = \{1, -1\}$, $iH = -iH\{i, -i\}$, $jH = -jH = \{j, -j\}$, $KH = -kH = \{K - K\}$
Example- $G = Q_4$, $H = \{\pm 1, \pm i\}$
$1H = -1H = iH = -iH = H$, $jH = -jH = kH = -kH = \{\pm j, \pm k\}$ then
H and jH are two distinct cosets of H in G.

Q. Find cosets of H in G when $H = \{I, (123), (132)\}$ and $G = S_3$
Solution: write by yourself.

No. of coset of H in $G = \frac{O(G)}{O(H)} = \frac{6}{3} = 2$.

[1] Lagrange's Theorem and Consequences

(i) If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$. Converse of Lagrange's need not be true.

(ii) $|a|$ divides $|G|$

(iii) Group of prime order are cyclic.

(iv) $a^{|G|} = e$

(v) Fermat's little theorem: For every integer *a* and every prime *p*, a^p modulo $\beta = a$ modulo *p*. (Important for questions)

Exam Point: Above five points are necessary to remember to do group theory. (Proofs of above points are not expected in exam).

Normal Subgroup: A subgroup H of G is said to be normal subgroup of g if $\forall x \in G, \forall h \in H$ $\Rightarrow xhx^{-1} \in H$ i.e. $xHx^{-1} = H$.

Q. If G is abelian then all subgroup of G are normal?
Proof: Let G be a abelian group and H is an subgroup of G
$\forall x \in G, \forall h \in H$ s.t $xhx^{-1} = x\left(hx^{-1}\right) = x\left(x^{-1}h\right), G = xx^{-1}h = eh = h \in H$; $xh^{-1}x \in H$
Then H is normal subgroup of G.

Example: $G = Z_{10}$ and $H = \langle 2 \rangle$ is subgroup of Z_{10} then H is normal subgroup of G.
Solution:
$G = Z_{10}$ is cyclic as well as abelian group . $H = \langle 2 \rangle = \{0, 2, 4, 6, 8\}$
Then H is normal subgroup of G because all subgroup of an abelian group are normal.

Q. $G = Z_2 \times Z_2$. How many normal subgroups in G?

Solution: $G = Z_2 \times Z_2$ is abelian group then all subgroups of G are normal.

Number of subgroups in $Z_2 \times Z_2$?

Number of cyclic subgroups of order 1 in $Z_2 \times Z_2$ = $\frac{\text{No. of elements of order 1 in } Z_2 \times Z_2}{\phi(1)}$

$= \frac{1}{1} = 1$

Number of cyclic subgroups of order 2 in $Z_2 \times Z_2 = \frac{\text{No. of elements of order 2 in } Z_2 \times Z_2}{\phi(2)} = \frac{3}{1} = 3$

$G = Z_2 \times Z_2$ itself is subgroup of $G = 1$

$H_2 = \{(0,0)\}$, $H_2 = \{(0,0),(0,1)\}$, $H_3 = \{(0,0),(1,0)\}$, $H_4 = \{(0,0),(1,1)\}$, $H_5 = Z_2 \times Z_2$

All are normal subgroups of $Z_2 \times Z_2$.

Q. How many normal subgroups in D_2 ?

Solution: $D_2 = \{R_0, R_{180}, f_{Aa}, f_{Bb}\}$. It is an abelian group $\therefore$ all its subgroups are normal subgroups of G

$O(D_2) = 4$ And D_2 has no elements of order 4 then D_2 is abelian but not cyclic.

Since D_2 is abelian then all subgroup of D_2 are normal.

$H_1 = \{R_0\}, H_2 = \{R_0, f_{Aa}\}, H_3 = \{R_0, f_{Bb}\}, H_4 = \{R_0, R_{180}\}, H_5 = D_2$

Q. $G = Z_4$, How many normal subgroups?

Solution: Z_4 is cyclic then Z_4 is abelian $\Rightarrow$ all subgroup of Z_4 are normal

Subgroup of Z_4 are $H_1 = \{0\} = \langle 4 \rangle, H_2 = \{0, 2\} = \langle 2 \rangle, H_3 = \langle 1 \rangle = Z_4$. All are normal subgroups of Z_4 .

Q. Show that $H = \{e\}$ and $H = G$ are always normal subgroup of G.

Solution: Case I: Let G be a group and $H = \{0\}$ is subgroup of G, $x \in G, h \in H = \{e\}$

s.t $xhx^{-1} = xex^{-1} = xx^{-1} = e \in H \Rightarrow xhx^{-1} \in H \Rightarrow H = \{e\}$ is normal subgroup of G.

Case II: Let G be a group and $H = G$ is subgroup of G, then $x \in G, h \in H = G$ s.t $xhx^{-1} \in H$ because

$x \in G, h \in H \Rightarrow h \in G \because (H = G) \Rightarrow xhx^{-1} \in G \Rightarrow xhx^{-1} \in H \ (G = H); \ xhx^{-1} \in H$

Then $H = G$ is normal subgroup of G.

Q. $G = D_4, H_1 = \{R_0\}$ and $H_2 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

H_1 and H_2 are normal subgroup of D_4 ?

Solution: $H_1 = \{R_0\}$ is the identity of D_4 and we know that $\{e\}$ is always normal subgroup of D_4 then $H = \{R_0\}$ is normal subgroup of D_4 and $H_2 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\} = D_4$ is normal subgroup in D_4 then H_1 and H_2 both are normal subgroup in D_4 .

Q.(i) $(Z+)$ is normal subgroup in $(Q+)$?

(ii) $(Q+)$ is normal subgroup in $(\mathbf{R},+)$?

(iii) $(Z,+)$ is normal subgroup in $(\mathbf{R},+)$?

Solution:(i) yes,(ii) yes,(iii) yes

Centre of Group

Let G be a group and $Z(G)$ is centre of group G then

$Z(G) = \{z \in G \mid xz = zx, \ \forall x \in G\}$.

Note- Centre of a group is a normal subgroup of that group, ….(1)

Let $x \in G$, and $h \in Z(G)$

$xhx^{-1} = (hx)x^{-1}$ [$h \in Z(G)$ then $hx = xh,\ \forall x \in G$] $= hxx^{-1} = he = h \in Z(G) \Rightarrow xhx^{-1} \in Z(G)$

$\therefore Z(G)$ is normal subgroup of G.

Q. $H = \{1, -1\}$ is subgroup of Q_4, H is normal subgroup in Q_4?

Solution:

$H = \{1, -1\}$ and $Z(Q_4) = \{1, -1\} = H$ and we know that $Z(G)$ is always normal subgroup of G then $H = \{1, -1\}$ is normal subgroup of Q_4.

Q. $G = GL_3(\mathbf{F}_7)$

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 4 & 0 \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix} \right\}$$

H is normal subgroup of G.

Solution:

$Z(GL_3(\mathbf{F}_7)) = H$ then H is a normal subgroup of $GL_3(\mathbf{F}_7)$.

Q. $H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} \right\}$

Is normal subgroup of $SL_3(\mathbf{F}_7)$?

Solution:

$Z(SL_3(\mathbf{F}_7)) = \gcd(3, 7-1) = 3$

$Z(SL_3(\mathbf{F}_7)) = H$ then H is normal subgroup of $SL_3(\mathbf{F}_7)$.

Q. Show that $SL_n(\mathbf{F})$ is normal subgroup of $GL_n(\mathbf{F})$?

Solution:

Let $x \in GL_n(\mathbf{F})$ and $h \in SL_n(\mathbf{F}) \Rightarrow |h| = 1$

$xhx^{-1} \in SL_n(\mathbf{F})$ because

$|xhx^{-1}| = |x||h||x^{-1}| = |x||x^{-1}| = |xx^{-1}| = |I| = 1.\ \ \therefore xhx^{-1} \in SL_n(\mathbf{F})$

Then $SL_n(\mathbf{F})$ is normal subgroup of $GL_n(\mathbf{F})$.

Q. Is $SL_2(\mathbf{F}_5)$ normal subgroup of $GL(\mathbf{F}_5)$?

Ans. Yes

Similarly, $SL_3(\mathbf{R})$ is normal subgroup of $GL_3(\mathbf{R})$.

Symmetric Group or Permutation Group

Definition: Set of all one-one onto mapping from set containing n elements to itself form a group under composition of functions. It is denoted by S_n and $O(S_n)=n!$ elements are called permutation of S_n.

Symmetric Group $S_1 : S_i = \{I\}, O(S_1)=1$

Group $S_2 ; S_2 = \{I, (1,2)\}$

Symmetric Group $S_3 ; S_3 = \{I, (12), (13), (23), (123)(132)\}$ $O(S_3)=6$

Cycle: A permutation $f \in S_n$ of length *r* is called *r*-cycle.

Transposition: A permutation of length 2 is called Transposition.

e.g. $f=(12)\in S_3$ and length of $f=2$, then *f* is called Transposition.

Example of *r*-cycle

$f=\begin{pmatrix} a_1a_2a_3.....a_{r-1}a_r \\ a_2a_3a_4.....a_ra_1 \end{pmatrix} \in S_n$; $a_i \neq a_j$, $i \neq j$ then length of $f=r$. *r*-cycle permutation.

$f\begin{pmatrix} 4\,2\,3 \\ 2\,3\,1 \end{pmatrix} \in S_4$, length of $f=3$, then 3-cycle.

Product of Two Permutation

$f_1=(123)\in S_3$, $f_2=(13)\in S_3$

$$f_1f_2=\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}\begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}=\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}=(23)$$

$$f=(12345)\in S_{n,n\geq5};\ f^2=f\cdot f=(12345)(12345)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}=(1\quad 3\quad 5\quad 2\quad 4)=(13524)$$

Order of Permutation:

$f \in S_n$ then $O(f)$ = length of *f*.

e.g.

$f=(123)\in S_4$, $O(f)=3$ = length of *f* then $O(f)=3$

$f=(123)\in S_4$, s.t. $f^2=(123)^2=(123)(123)=(132)$

Now, $f^3=(132)(123)=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}=I$

Q. $f=(123)(45)\in S_6$ $O(f)=?$

Solution: $f=(123)(45)=f_1\cdot f_2$

$f^2=f_1^2\cdot f_2^2=(132)\cdot I=(132)$, $f^3=f_1^2 f_2=I\cdot(45)$

$f^4=f_1^3 f_2=(123)I=(123)$, $f^5=f^4\cdot f=(132)\cdot(45)$

$f^6=I\cdot I=I=f^5\cdot f=(132)(45)(128)(45)$. So $O(f)=6$

Q. $f=(123)(145)\in S_n$, find $O(f)=?$

Solution: $f=(123)(145)=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&4&5\\4&5&1\end{pmatrix}=\begin{pmatrix}1&4&5&2&3\\4&5&2&3&1\end{pmatrix}=(1\quad 4\quad 5\quad 2\quad 3)$

Then $O(f)=5$.

- $f=f_1\cdot f_2\cdot f_3$

Where $f_1=\begin{pmatrix}a_1&a_2&a_3&a_4\\a_2&a_3&a_4&a_1\end{pmatrix}, f_2=\begin{pmatrix}a_5&a_6\\a_6&a_5\end{pmatrix}, f_3=\begin{pmatrix}a_7&a_8&a_9\\a_8&a_9&a_7\end{pmatrix}$

$O(f)=\text{L.C.M.}(O(f_1),O(f_2),O(f_3))$

Where f_1, f_2, f_3 are distinct permutation.

Exam Point: If $f=f_1, f_2,....,f_k$, where $f_1, f_2,....,f_k$ are distinct permutation.

Then $O(f)=\text{LCM}(O(f_1),O(f_2)....O(f_k))$

Q. $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&1&6&5&8&9&7\end{pmatrix}\in S_{n,n\geq 9}$ the $O(f)$?

Solution:

$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&1&6&5&8&9&7\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}5&6\\6&5\end{pmatrix}\begin{pmatrix}7&8&9\\8&9&7\end{pmatrix}$

$=f_1\cdot f_2\cdot f_3$

$\Rightarrow O(f)=\text{L.C.M.}(O(f_1),O(f_2),O(f_3))=\text{L.C.M.}(4,2,3)\therefore O(f)=12$

Q. $f=(123)(145)\in S_n$, find $f^{99}=?$

Solution: $f=(123)(145)=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}\begin{pmatrix}1&4&5&2&3\\4&5&1&2&3\end{pmatrix}=\begin{pmatrix}1&4&5&2&3\\4&5&2&3&1\end{pmatrix}$

$f=(1\quad 4\quad 5\quad 2\quad 3)\Rightarrow O(f)=5\Rightarrow f^5=I$

$f\cdot f=f^2=\begin{pmatrix}1&4&5&2&3\\4&5&2&3&1\end{pmatrix}\begin{pmatrix}1&4&5&2&3\\4&5&2&3&1\end{pmatrix}=\begin{pmatrix}1&4&5&2&3\\5&2&3&1&4\end{pmatrix}=(1\quad 5\quad 3\quad 4\quad 2)$

$f^{99}=f^{95+4}=f^4=f^2\cdot f^2$

$f^2=\begin{pmatrix}1&5&3&4&2\\5&3&4&2&1\end{pmatrix}=(1\quad 5\quad 3\quad 4\quad 2)$

$f^4=\begin{pmatrix}1&3&2&5&4\\3&2&5&4&1\end{pmatrix}=f^2\cdot f^2$

$f^4=(1\quad 3\quad 2\quad 5\quad 4)$

or $f^{99}=f^{100}f^{-1}=(f^5)^{20}\cdot f^{-1}=I\cdot f^{-1}=f^{-1}$

$f^{99}=f^4=(3\quad 2\quad 5\quad 4\quad 1)$

Inverse of Permutation

$f = (a_1, a_2 .....a_k) \in S_n$

$f^{-1} = (a_k a_{k-1} ....a_2 a_1)$ s.t $ff^{-1} = I$

Q. $f = (1 \quad 2 \quad 3 \quad 4) \in S_n$ then $f^{-1} = (4 \quad 3 \quad 2 \quad 1)$?

Solution: $ff^{-1} = (1 \quad 2 \quad 3 \quad 4)(4 \quad 3 \quad 2 \quad 1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I$

$ff^{-1} = I$

Even Permutation: A permutation $f \in S_n$ is called an even permutation if *f* can be written as product of even number of transpositions.

e.g. $(123) \in S_4$, is even permutation?

Solution: $f = (123) \in S_4 = (13)(12)$

Even no. of transposition then $f = (123)$ is an even permutation.

Q. $f = (123456) \in S_6$, is this even permutation?

Solution: $f = (123456) = \dfrac{(16)(15)(14)(13)(12)}{5 - \text{transposition}}$. Thus $f = (123456)$ is not even permutation.

Odd Permutation: A permutation $f \in S_n$ is called an odd permutation if f can be written as product of odd number of transposition.

e.g. $f = (1234) \in S_5$ is odd permutation

Solution: $f = (1234) = (14)(13)(12)$, so it is an odd permutation as there are 3.

So, $f = (1234)$ is an odd permutation.

Exam Point: $I \in S_n$ is always an even permutation

$$I = \underbrace{(12)(12)(12)(12)(12)(12)}_{\text{even no.of transpositions}}$$

Then I is an even permutation.

$I = (12)(12),\ I \in S_n,\ \forall n \in N$

$I = (12)(12)(12)(12)$

$I = (12)(12).....$ even times

Then I is an even permutation also $I \in S_1$ is even permutation.

Exam Point: (1) Product of two even permutation is an even permutation.

(2) Product of two odd permutation is an even permutation.

(3) Product of odd and even permutation is an odd permutation.

e.g.

(1) $f = (123)$ is even permutation ; $f \cdot f = (123)(123) = (132) = (12)(13)$ = even permutation

(2) $f_1 = (123)$ and $f_2 = (23)$; $f_1 \cdot f_2 = (123)(23) = (13)(12)(23)$ = odd permutation

(2) $f_1 = (12)$ $f_2 = (13)$; $f_1 \cdot f_2 = (12)(13)$ = even permutation

Q. (i) If $f \in S_n$ is an even permutation then f^{-1} is an even permutation.

(ii) If $f \in S_n$ is an odd permutation then f^{-1} is an odd permutation.

Solution:

(i) Let $f \in S_n$, f is an even permutation

$ff^{-1} = I$ — even Permutation

f is even permutation

$\because f$ is an even permutation given and we know that I is always even permutation then f^{-1} must be even because product of even permutation is even

$\Rightarrow f^{-1}$ is even permutation

If f^{-1} is odd then even + odd = odd $\neq$ even

Then f^{-1} = even is not possible $\Rightarrow f^{-1}$ is an even permutation

Proof: (ii) Given $f \in S_n$ is odd permutation

We know that

$ff^{-1} = I$. And I is always even permutation and for validation of this result f^{-1} must be odd because product of two odd permutation is even. $\therefore f^{-1}$ is odd permutation.

Q. $f = \alpha\beta\alpha^{-1}\beta^{-1}$ is always an even permutation.

Solution:

$\alpha \in S_n$ then α is either even or odd permutation, $\beta \in S_n$ then β is either even or odd permutation.

Case – I: If α =even and β = even permutation α is an even permutation then α^{-1} is also even permutation. Similarly β is an even permutation then β^{-1} is also even permutation.

$f = \alpha\beta\ \alpha^{-1}\beta^{-1}$

even even

Case – II: If α is an odd permutation and β is an odd permutation

$\Rightarrow \alpha^{-1}$ and β^{-1} both are also odd permutation. $\alpha\beta$ is even permutation

$\alpha^{-1}\beta^{-1}$ is even permutation

$f = (\alpha\beta)\cdot(\alpha^{-1}\beta^{-1})$ = even • even = even permutation

Case – III: When α is even and β is odd permutation

α^{-1} will be even permutation and β^{-1} will be permutation .

$\alpha\beta$ will be odd permutation, $\alpha^{-1}\beta^{-1}$ will be odd permutation

i.e. $f = (\alpha\beta)(\alpha^{-1}\beta^{-1})$ = odd • odd = even permutation

Case – IV: When α is odd $\Rightarrow \alpha^{-1}$ is odd permutation

β is even $\Rightarrow \beta^{-1}$ is even permutation

$\alpha\beta$ is odd permutation, $\alpha^{-1}\beta^{-1}$ is also odd permutation

$f = (\alpha\beta)(\alpha^{-1}\beta^{-1})$ = odd • odd = even permutation

Hence, $f = \alpha\beta\alpha^{-1}\beta^{-1}$ is always an even permutation.

Q. (i) $f = \alpha\beta\alpha^{-1} \in S_n$, always even permutation when β is even.

(ii) $f = \alpha\beta\alpha^{-1} \in S_n$, always odd permutation is β is odd.

Exam Point: No. of distinct permutation of length *r* in $S_n = \frac{1}{r}\frac{n!}{(n-r)!}$

Proof: No. of distinct arrangement of *r* number out or *n* number ${}^nP_r = \frac{n!}{(n-r)!}$

But $(1,2,3,....r) = (2\cdot 3.....r\cdot 1) = (3\cdot 4....r\cdot 1\cdot 2) = (r\cdot 1\cdot 2.....r-1)$

are same permutation in S_n. $\therefore$ # of distinct arrangement of *r*-cycles in $S_n = \frac{n!}{r(n-r)!}$

Q. Find number of Permutation in S_3 of length 2.

Solution:

Number of permutations of length 2 in $S_3 = \frac{3!}{2(3-2)!} = \frac{3\cdot 2\cdot 1}{2\cdot 1} = 3$

Those are $(12),(13),(23) \in S_3$

Q. How many permutations of length 3 in S_4 or number of 3-cycle in S_4?

Solution:

number of 3-cycles in $S_4 = \frac{4!}{3(4-3)!} = \frac{4\times \cancel{3}\times 2\times 1}{\cancel{3}} = 4\times 2 = 8$

Q. How many elements of order 2 in S_4?

Solution: Elements of S_4: $O(S_4) = 4! = 24$

$$S_4 = \left\{\begin{matrix} I\,(12),(13),(14),(23),(24),(34),(123) \\ (124),(234),(134),(431),(432),(421) \\ (321),(1234),(1243),(1423),(3241) \\ (3421),(4321),(12)(34),(14)(23),(13)(24) \end{matrix}\right\}$$

$(12)\in S_4$ s.t $O(12)=2$, $(13)\in S_4$ s.t $O(13)=2$, $(24)\in S_4$ s.t $O(14)=2$

$(23)\in S_4$ s.t $O(23)=2$, $(24)\in S_4$ s.t $O(24)=2$, $(34)\in S_4$ s.t $O(34)=2$

$(12)(34)\in S_4$ s.t $O((12)(34))=2$, $(14)(23)\in S_4$ s.t $O((14)(23))=2$

$(13)(24)\in S_4$ s.t $O((13)(24))=2$

Therefore number of elements of order 2 in S_4 is = 9.

Q. (i) Find number of element or order 2 in S_6.

(ii) Find number of element of order 3 in S_6.

Q. How many elements of order 3 in S_4.

Solution: Number of elements of order 3 in S_4 are

$\{(123),(124),(134),(234),(432),(431),(421),(321)\}$; exactly 8 elements or order 3 in S_4.

Q. How many elements of order 4 in S_4?

Solution: $\{(1234),(1243),(1423),(3241),(3421),(4321)\}$

exactly 6 elements of order 4.

Permutation	No. of subgroup
S_1	1
S_2	2
S_3	6
S_4	30
S_5	156

Note: Number of elements of order 'd' in S_n

$$=\frac{\Sigma\underline{|n}}{1^{\alpha_1}\cdot 2^{\alpha_2}....k^{\alpha_k}\underline{|\alpha_1}\underline{|\alpha_2}.....\underline{|\alpha_k}}$$

where α_i is equal to number of i's in the selected partition and L.C.M. $(1,2,.....k)=d$

Q. Find number of elements of order 1 in S_4.

Solution:

$G=S_4$

$4\to$ $LCM(4)=4$, elements of order 4

3+1$\to$ $LCM(3,1)=3$, elements or order 3

2+2 $\to$ $LCM(2,2)=2$, elements of order 2

2+1+1 $\to$ $LCM(2,1,1)=2$, elements of order 2

1+1+1+1$\to$ $LCM(1,1,1,1)=1$, elements or order 1

No. of elements of order 1 in $S_4(1+1+1+1)$

$$=\frac{\underline{|4}}{1^4\cdot 2^\circ\cdot 3^\circ\cdot 4^\circ\underline{|4}\,\underline{|0}\,\underline{|0}\,\underline{|0}}=\frac{\cancel{\underline{|4}}}{1\cdot\cancel{\underline{|4}}}=1$$

Q. Find no of elements of order 2 in S_4.

Solution:

$G=S_4$

The partition 2+2 and 2+1+1 gives elements or order 2 in S_4.

(i) No. of elements or order 2 in S_4 corresponding to partition

$$(2+2)=\frac{\underline{|4}}{1^\circ\cdot 2^\circ\cdot 3^\circ\cdot 4^\circ\cdot\underline{|0}\,\underline{|2}\,\underline{|0}\,\underline{|0}}$$

$$=\frac{\underline{|4}}{4\cdot\underline{|2}}=\frac{4\times 3\times\cancel{\underline{|2}}}{4\cancel{\underline{|2}}}=\frac{1\cancel{2}}{\cancel{4}}=3$$

$f=(12)(34),(13)(24),(14)(23)=3$ there are the elements or order 2.

(ii) No. of elements of order 2 in S_4 corresponding to partition

$$(2+1+1)=\frac{\underline{|4}}{1^2\cdot 2^1\cdot 3^\circ\cdot 4^\circ....k^\circ\underline{|2}\,\underline{|1}\,\underline{|0}\,\underline{|0}}$$

$$=\frac{\underline{|4}}{2\cdot\underline{|2}}=\frac{4\times 3\times\cancel{\underline{|2}}}{2\times\cancel{\underline{|2}}}=6$$

$f=(12),(13),(14),(23),(24),(34)=6$

Total No. of elements of order 2 in $S_4=3+6=9$.

Q. Find No. of elements or order 3 in S_4?

Solution:

$G=S_4$

4

3+1 $\rightarrow$ LCM (3,1) = 3

2+2

2+1+1

1+1+1+1

# of elements of order 3 in $S_4=\frac{\underline{|4}}{1^1 2^\circ 3^1\underline{|1}\,\underline{|0}\,\underline{|1}}=\frac{\underline{|4}}{3\cdot 1\cdot 1}=\frac{4\times\cancel{3}\times 2\times 1}{\cancel{3}}=8$

Q. Find No. of elements of all possible order in S_5.

Solution:

$G=S_5$

$5\rightarrow LCM(5)=5$

$4+1\rightarrow LCM(4,1)=4$

$3+2\rightarrow LCM(3,2)=6$

$3+1+1\rightarrow LCM(3,1,1)=3$

$2+2+1\rightarrow LCM(2,2,1)=2$

$2+1+1+1 \rightarrow LCM(2,1,1,1)=2$

$1+1+1+1+1 \rightarrow LCM(1,1,1,1,1)=1$

Possible order of elements in S_5 are 1,2,3,4,5 and 6.

Q. Find No. of elements of order 2 in S_5?

Solution:

$G = S_5$

$2+2+1 \rightarrow LCM(2,2,1)=2$

$2+1+1+1 \rightarrow LCM(2,1,1,1)=2$

(i) No. of elements of order 2 w.r.t. partition

$$(2+2+1) = \frac{\underline{|5}}{1^1 \cdot 2^2 \cdot 3^0 \ldots k^0 \underline{|1}\,\underline{|2}\,\underline{|0}} = \frac{\underline{|5}}{1 \cdot 4 \cdot \underline{|2}}$$

$$= \frac{5\times4\times3\times \not{2}\times1}{4\times\not{2}\times1} = 15$$

(ii) No. of elements of order 2 w.r.t. partition (2+1+1+1)

$$= \frac{\underline{|5}}{1^3 \cdot 2^1 \cdot 3^0 \ldots \underline{|3}\,\underline{|1}\,\underline{|0}} = \frac{5\times4\times\not{3}\times\not{2}\times1}{1\times2\times1\times\not{3}\times\not{2}\times1} = 10$$

Total elements of order 2 in S_5 is = 15+10 = 25

# of elements of order 3 in S_5?

Solution:

$G = S_5$

$3+1+1 \rightarrow LCM(3,1,1)=3$

No. of elements of order 3 in $S_5(3+1+1)$

$$= \frac{\underline{|5}}{1^2 \cdot 2^0 \cdot 3^1 \underline{|2}\,\underline{|1}\,\underline{|0}} = \frac{5\times4\times\cancel{3\times2\times1}}{\cancel{3\times2\times1}} = 20$$

Q. No. of elements or order 4 in S_5?

Solution:

$G = S_5$

$4+1 \rightarrow LCM(4,1)=4$

No. of elements of order 4 in $S_5(4+1)$

$$= \frac{\underline{|5}}{1^1 \cdot 2^2 \cdot 3^0 \cdot 4^1 \underline{|1}\,\underline{|0}\,\underline{|0}\,\underline{|1}} = \frac{5\times\not{4}\times3\times2\times1}{\not{4}\times1\times1} = 30$$

Q. No. of elements of order 5 in S_5?

Solution:

$5 \rightarrow LCM(5)=5$

# of elements of order 5 in $S_5(5) = \dfrac{\underline{|5}}{1^\circ \cdot 2^\circ \cdot 3^\circ \cdot 4^\circ \cdot 5^\circ \underline{|0}\,\underline{|0}\,\underline{|1}} = \dfrac{\not{5}\times4\times3\times2\times1}{\not{5}} = 24$

# of elements of order 6 in $S_5(3+2) = \dfrac{\lfloor 5}{1^0 \cdot 2^1 \cdot 3^1 \cdot 4^0 \lfloor 1 \lfloor 1 \lfloor 0} = \dfrac{5\times 4\times \cancel{3\times 2}\times 1}{\cancel{2\times 3}} = 20$

Total No. of elements $= 1+25+20+30+24+20 = 120$

Q. How many elements of order 2 in S_6?

$2+2+2 \to LCM(2+2+2) = 2$

$2+2+1+1 \to LCM(2,2,1,1) = 2$

$2+1+1+1+1 \to LCM(2,1,1,1,1) = 2$

# of elements of order 2 in respect of partition $(2+2+2)$

$= \dfrac{\lfloor 6}{2^3 \cdot \lfloor 3}$

$= \dfrac{36\times 5\times 4\times \sqrt{3}}{28\lfloor 3} = 15$

# of elements of order 2 w.r.t. $(2+2+1+1)$

$= \dfrac{\lfloor 6}{2^2 \cdot 1^2 \cdot \lfloor 2 \lfloor 2} = \dfrac{6\times 5\times \cancel{4}\times 3\times \cancel{\lfloor 2}}{\cancel{\lfloor 2}\,\cancel{\lfloor 2}\,\cancel{4}} = 45$

# of elements of order 2 w.r.t. $(2+1+1+1+1)$

$= \dfrac{\lfloor 6}{1^4 \cdot 2^1 \cdot \lfloor 4 \lfloor 1} = \dfrac{6\times 5\times \lfloor 4}{2\times \lfloor 4} = 15$

Total elements in $S_6 = 15+45+15 = 75$

Q. $\beta = (1357986)(2410) \in S_{10}$, find smallest positive integer *m*, such that $\beta^m = \beta^{-5}$.

Solution:

$\beta = (1,3,5,7,9,8,6)(2,4,10)$

$\beta = \beta_1 \cdot \beta_2$ where $\beta_1 = (1,3,5,7,9,8,6)$, $\beta_2 = (2,4,10)$

$O(\beta) = LCM(O(\beta_1), O(\beta_2))$

$= LCM(7,3) = 21 \Rightarrow O(\beta) = 21$

$\beta^{21} = I$

$\beta^{21} \cdot \beta^{-5} = I \cdot \beta^{-5}$

$\beta^{16} = \beta^{-5}$

i.e. $\beta^m = \beta^{16} = \beta^{-5}$

$\Rightarrow m = 16$

Q. $\alpha = (13579)(246)(8,10)$ and a^m is 5-length, find possibility of *m*.

Solution:

$\alpha = (13579)(246)(810)$

where $\alpha_1 = (13579), \alpha_2 = (246), \alpha_3 = (810)$

$= \alpha_1 \alpha_2 \alpha_3$

$O(\alpha) = L.C.M.\left(O(\alpha_1), O(\alpha_2), O(\alpha_3)\right)$

$= L.C.M.(5,3,2) = 30$

$\Rightarrow O(\alpha) = 30$

i.e. $\alpha^{30} = I$, On squaring α_2 it becomes identity and α_3 becomes identity on cubing.

$\alpha^6 = (13579)\cdot I = (13579)$

$\alpha^{12} = (15937)$

$\alpha^{18} = (17395)$

$\alpha^{24} = (19753)$

$\therefore$ Possibility of m are, $m = 6, 12, 18, 24$

i.e. multiple of 6 but $m < 30$ because $\alpha^{30} = I$

Q. In S_3, find α and β s.t. $|\alpha| = 2, |\beta| = 2$ and $|\alpha\beta| = 3$, i.e. $O(\alpha) = 2, O(\beta) = 2$ and $O(\alpha\beta) = 3$.

Solution:

$S_3 = \{I, (12), (13), (23), (123), (132)\}$

$\alpha = (12) \Rightarrow |\alpha| = 2$

$\beta = (13) \Rightarrow |\beta| = 2$

$\alpha\beta = (12)(13) \Rightarrow (\alpha\beta) = (132)$

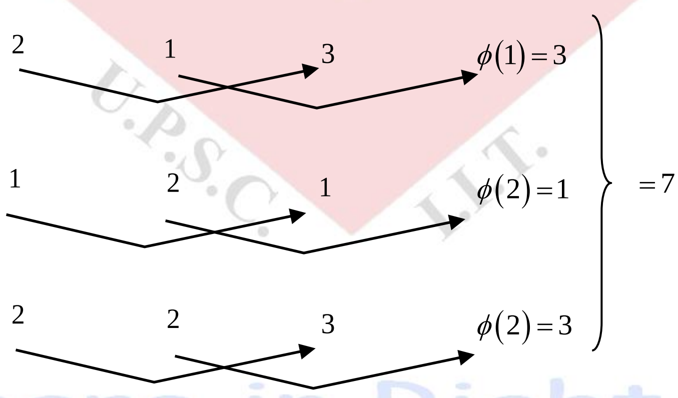
$\Rightarrow |\alpha\beta| = 3$

i.e. $O(\alpha) = 2, O(\beta) = 2$ and $O(\alpha\beta) = 3$.

Q. How many elements of order 2 in $S_3 \times Z_2$.

Solution:

$G = S_3 \times Z_2$



Q. How many elements of order 2 in $S_4 \times Z_2$?

Solution:

$G = S_4 \times Z_2$

$2 \quad 1 \Rightarrow 9 \cdot \phi(1) = 9$

$1 \quad 2 \Rightarrow 1 \cdot \phi(2) = 1$

$2 \quad 2 \Rightarrow 9 \cdot \phi(2) = 9$

Total = 19

then # of elements of order 2 in $S_4 \times Z_2 = 19$.

Q. How many elements of order 2 in $S_4 \times Z_3$?

Solution:

$G = S_4 \times Z_3$

$2 \quad 1 \rightarrow 9 \cdot \phi(1) = 9$

# of elements of order 2 in $S_4 \times Z_4 = 9$.

Alternating Group (A_n):

$A_n = \{$Set of all even Permutation of $S_n\}$

Show that A_n is a group w.r.t Composition.

Proof: $A_n \subseteq S_n$, we have to show that $(A_n, 0)$ is a group.

(1) Let, $x \in A_n \Rightarrow x$ is an even permutation

and $y \in A_n \Rightarrow y$ is an even permutation.

$xy =$ even permutation (Product 2 even permutation is even permutation)

Closure property satisfied.

(2) $\forall x \in A_n$, $\exists I \in A_n$ because I is an even permutation s.t. $x \cdot I = I \cdot x = x$

(3) If $x \in A_n$, then *x* is even permutation

$\Rightarrow x^{-1}$ is also even permutation then $x^{-1} \in A_n$

$\Rightarrow xx^{-1} = x^{-1}x = I$

then A_n is group w.r.t. to composition and

$$O(A_n) = \frac{O(S_n)}{2} = \frac{\lfloor n}{2};\ n \geq 2$$

Note: $O(S_n) = O(A_n)$, when $n = 1$

$$O(A_n) = \frac{O(S_n)}{2} = \frac{n!}{2};\ n \geq 2$$

(i) $A_1 = \{I\}$, $O(A_1) = 1$

(ii) $A_2 = \{I\}$, $O(A_2) = 1$ because $S_2 = \{I, (12)\}$, I is even permutation only.

(iii) $S_3 = \{I, (12), (13), (23), (123), (132)\}$

$A_3 = \{I, (123), (132)\}$

$$O(A_3) = \frac{O(S_3)}{2} = \frac{\lfloor 3}{2} = 3$$

(iv)

$$S_4 = \left\{\begin{array}{l} I,(12),(13),(23),(24),(34) \\ (14),(123),(124),(234),(134) \\ (432),(431),(421),(321), \\ (1234),(1243),(1423),(3241) \\ (3421),(12)(34),(14)(23),(13)(24) \end{array}\right\}$$

$$A_4 = \{I,(123),(124),(134),(234),(432),(431),(421),(321),(12)(34),(14)(23),(13)(24)\}$$

$$\therefore O(A_4) = \frac{O(S_4)}{2} = \frac{24}{2} = 12$$

Possible order of elements in A_4 are 1,2,3.

Number of elements of order 1 in $A_4 = 1$

Number of elements of order 2 in $A_4 = 3$

Number of elements of order 3 in $A_4 = 8$

Total = 12. also $O(A_4) = 12$

S_4, for A_4, odd permutation not selected $4 \rightarrow$ odd permutation × 3+1 $\rightarrow$ even + even = even permutation √ $2+2 \rightarrow$ odd + odd = even permutation √ $2+1+1 \rightarrow$ odd + even + even = odd permutation × $1+1+1+1 \rightarrow$ even + even + even + even = even permutation √

Q. Find no of elements of possible order in A_5?

Solution:

$G = A_5$

$5 \rightarrow$ even permutation √	5
$4+1 \rightarrow$ odd = odd + even ×	4
$3+2 \rightarrow$ odd = even + odd ×	6
$2+2+1 \rightarrow$ even = even + even + even √	2
$3+1+1 \rightarrow$ even = even + even + even √	3
$2+1+1+1 \rightarrow$ odd = odd + even + even + even	2
$1+1+1+1+1 \rightarrow$ even = even + even + even + even + even √	

$LCM(5) = 5,\ LCM = (3,1,1) = 3$

$LCM(2,2,1) = 2,\quad LCM(1,1,1,1,1) = 1$

Possible order of elements in A_5 are 1,2,3 and 5

number of elements of order 1 in $A_5(1+1+1+1+1) = \frac{\lfloor 5}{1^5 \lfloor 5} = 1$

number of elements of order 2 in $A_5(2+2+1) = \frac{\lfloor 5}{2^2 \cdot 1 \lfloor 2} = \frac{5 \times \cancel{4} \times 3 \times \cancel{2} \times 1}{\cancel{4} \times 1 \times \cancel{2}} = 15$

number of elements of order B in $A_5 = (3+1+1) = \dfrac{\underline{|5}}{1^2 \cdot 3\underline{|2}\underline{|1}} = \dfrac{5\times 4\times \cancel{3\times 2}\times 1}{\cancel{3\times 2}\times 1\times 1} = 20$

number of elements of order 5 in $A_5(5) = \dfrac{\underline{|5}}{5\underline{|1}} = \dfrac{\cancel{5}\times 4\times 3\times 2\times 1}{\cancel{5}} = 24$

Total number of elements in $A_5 = 1+15+20+24 = 60$.

Q. How many elements of order 4 in $A_5 \times Z_3$.

Ans. Neither A_5 nor Z_3 has elements of order 4 so no element exists of order 4 in $A_5 \times Z_3$.

Q. Set of all odd permutation of S_n is a group?

Solution:

$S = \{$Set of all odd permutation of $S_n\}$

$x \in S$, then x is odd permutation, $y \in S$, then y is odd permutation

$xy \in S$ even permutation then $xy \notin S$. $\Rightarrow S$ is not group w.r.t composition.

Closure property not satisfied.

Exam Point:

(i) $Z(S_n)_{n\geq 3} = \{I\}$

(ii) $Z(A_3) = A_3$

(iii) $Z(A_n) = \{I\}$, if $n \geq 4$

Q. Show that A_n is normal subgroup of S_n, $n \geq 2$.

Proof: A_n is subgroup of S_n and

$$i_{S_n}(A_n) = \frac{O(S_n)}{O(A_n)} = \frac{\underline{|n}}{\frac{\underline{|n}}{2}} = 2$$

then $i_{S_n}(A_n) = 2 \Rightarrow A_n$ is normal subgroup of S_n.

Exam Point:

: $S_n, n \neq 4$, only normal subgroups are

$H_1 = \{I\}, H_2 = A_n, H_3 = S_n$

If $n = 1$, then $H_1 = H_2 = H_3$

If $n = 4$, then $H_1 = \{I\}$, $H_2 = \{I(12)(34)(13)(24),(14)(23)\}$ then normal subgroup in A_4 are $H_3 = A_4, H_4 = S_4$.

Exam Point:

: A_n, $n \neq 4$ only normal subgroups are $H_1 = \{I\}, H_2 = A_n$.

If $n = 4$ then same as S_n for $n = 4$.

Q. If $H = \{I, (12)(34), (13)(24), (14)(23)\}$ is normal subgroup in S_4 then show that H is normal in A_4.

Solution:

$H \subseteq A_4 \subseteq S_4$, and H is normal subgroup in S_4 and $A_4 \subseteq S_4$ then H is normal subgroup in A_4.

Factor Group of S_3

Solution: $H_1 = \{I\}, H_2 = A_3, H_3 = S_3$ are Normal subgroup in S_3.

(i) $\frac{S_3}{H_1} = \frac{S_3}{\{I\}} \approx S_3$ factor group

(ii) $\frac{S_3}{H_2} = \frac{S_3}{A_3} = \{aA_3 | a \in S_3\}$

$$O\left(\frac{S_3}{A_3}\right) = 2$$

$A_3 = \{I (123), (132)\}$ then,

$$S_3 = \{I \cdot A_3, (12) A_3\}$$

$$A_3 = \{A_3, (12) A_3\}$$

$$\frac{S_3}{A_3} \approx Z_2$$

(iii) $\frac{S_3}{S_3} = \{aS_3 | a \in S_3\}$

$$\frac{S_3}{S_3} \approx Z_1$$

Factor Group of S_4

Solution: Normal subgroup of S_4 are

$$H_1 = \{I\}, H_2 = A_4, H_3 = S_4$$

$$H_4 = \{I, (12)(34), (13)(24), (14)(23)\}$$

(i) $\frac{S_4}{H_1} = \frac{S_4}{\{I\}} \approx S_4$

(ii) $\frac{S_4}{H_2} = \frac{S_4}{A_4} = \{aA_4 | a \in A_4\}$

$$= \{I \cdot A_4, (12) A_4\}$$

$$\frac{S_4}{A_4} \approx Z_2$$

(iii) $\frac{S_4}{H_3} = \frac{S_4}{S_4} = \{aS_4 | a \in S_4\}$

$\frac{S_4}{S_4} \approx Z_1$

(iv) $\frac{S_4}{H_4} = \frac{S_4}{H_4} = \{aH_4 | a \in S_4\} \approx S_3$

$\therefore \frac{S_4}{H_4} \approx S_3$

$O\left(\frac{S_4}{H_4}\right) = \frac{24}{4} = 6$

If $\frac{S_4}{H_4} \approx Z_6$ then $\frac{S_4}{H_4}$ has elements of order 6 then S_4 has elements of order 6 but S_4 has no element of order 6 then

$\frac{S_4}{H_4} \approx S_3$.

Factor Group of S_7

Normal Subgroup of S_7:

$H_1 = \{I\}, H_2 = A_7$

$H_3 = S_7$

(1) $\frac{S_7}{\{I\}} \approx S_7$

(2) $\frac{S_7}{A_7} = \{aA_7 | a \in A_7\} = \{I \cdot A_7, (12)A_7\} \approx Z_2$

(3) $\frac{S_7}{S_7} = \{aS_7 | a \in S_7\} = \{I\} \approx Z_1$

i.e. $\frac{S_7}{\{I\}} \approx S_7$, $\frac{S_7}{A_7} \approx Z_2$, $\frac{S_7}{S_7} \approx Z_1$

Factor Group of A_n

(i) $n = 4$ then

$A_4 = \{I(123),(124),(134),(234),(432),(431),(421),(321)(12)(34),(13)(24),(14)(23)\}$

Normal subgroup of A_4 **are**:

$H_1 = \{I\}, H_2 = \{I,(12)(34),(13)(24),(14)(23)\}$

$H_3 = A_4$

(1) $\frac{A_4}{H_1} = \{a \cdot H_1 | a \in A_4\}$

$\frac{A_4}{H_1} \approx A_4$

(2) $\frac{A_4}{H_2} = \{aH_2 \,|a \in A_4\} \approx Z_3$

(3) $\frac{A_4}{H_3} = \frac{A_4}{A_4} \approx Z_1$.

Q. How many subgroups of order 4 in A_4? And it is isomorphic to?
Solution:
A_4 has 3 elements of order 2 and no elements of order 4 in A_4.
$\therefore$ No cyclic subgroup exists
$H_2 \approx Z_2 \times Z_2$
$\therefore$ Unique subgroup of order 4 in A_4.

Q. Maximum order of elements in S_{10}.
(1) 10 (2) 21 (3) 30 (4) 60
Solution:
In Partition $(2+3+5)$ of S_{10}
L.C.M. $(2,3,5) = 30$
In S_{10} max. order of any element = 30
w.r.t partition $(2+3+5)$

Q. Maximum order of element in A_{10}?
(1) 10 (2) 21 (3) 30 (4) 60
Solution:
10 = 2+3+5 $\rightarrow$ Odd Permutation = LCM (2,3,5) = 30
10 =7+3$\rightarrow$ even permutation LCM (7,3) = 21

SIMPLE GROUP: A group G is said to be simple group if G has only normal subgroups as $H = \{e\}$ and $H = G$ itself.
e.g. $G = Z_{11}$, G is simple?
Solution:
$G = Z_{11}$, has exactly two subgroup
$H_1 = \{0\}, H_2 = Z_{11}$
Since, Z_{11} is cyclic then H_1 and H_2 are normal subgroup of Z_{11}.
Then, $G = Z_{11}$ is simple.
Q. $G = D_4$ is simple?
Solution:
No, because $H_1 = \{R_0, R_{180}, H, V\}$
$H_2 = \{R_0, R_{180}, D, D'\}$
$H_3 = \{R_0, R_{180}\}$
are normal subgroup in D_4 then D_4 is not simple.

Q. $G = Z_4$, is this simple?

Solution:

Z_4 is cyclic group then all subgroup of Z_4 are normal subgroup.

Subgroup in Z_4 are

$H_1 = \{0\}, H_2 = \langle 2 \rangle = \{0, 2\}$

$H_3 = Z_4$, thus Z_4 is not simple.

Q. A_3 is simple?

Ans. Normal subgroup of A_3 are $H_1 = \{I\}$, $H_2 = A_3$ thus A_3 is simple.

Q. S_3 is simple?

Ans. No, because normal subgroup of S_3 are

$H_1 = \{I\}, H_2 = A_3, H_3 = S_3$ thus S_3 is not simple.

Q. D_3 is simple?

Ans. No, because normal subgroups of D_3 are

$D_3 = \{R_0, R_{120}, R_{240}, f_{Aa}, f_{Bb}, f_{Cc}\}$

$H_1 = \{R_0\}, H_2 = \{R_0, R_{120}, R_{240}\}$

$H_3 = D_3$

Q. Show that $H = \{R_0, f_{Aa}\}$ is not normal subgroup in D_3?

Solution:

$x = R_{120}$, $h = f_{Aa}$

$R_{120} f_{Aa} R_{120^{-1}}$

$= R_{120} f_{Aa} R_{240}$

$= R_{120} \cdot f_{Cc}$

$= f_{Bb} \notin H$

Here, $R_{120} \cdot f_{Aa} R_{120^{-1}} \notin H$ i.e. $f_{Bb} \notin H$ then H is not normal subgroup of D_3.

Q. $G = S_n$, $n \geq 3$, G is simple?

Solution: No, because it will have more than two normal subgroup other than $\{e\}$ and G i.e. A_n

Q. $A_n, n \geq 5$ is this simple?

Solution: Normal subgroup in $A_n, n \geq 5$ are $H = \{I\}$ and $H = A_n$, then A_n is simple this is the smallest non-abelian simple group.

Q. A_4 is not simple?

Ans. Yes, because normal subgroup of A_4 are

$H = \{I\}$, $H = A_4$, $H = \{I(12)(34),(13)(24),(14)(23)\}$

Homomorphisms

Let $(G_1, 0)$ and $(G_2, *)$ are two groups A mapping $f : (G_1, 0) \to (G_2, *)$ is homomorphism if

$f(x \circ y) = f(x) * f(y);\ x, y \in G_1,\ f(x), f(y) \in G_2$

e.g.

Q. $f : Z_4 \to Z_{10}$ defined by $f(x) = 0 \cdot x$ is homomorphism?

Solution:

$f : Z_4 \to Z_{10}$

$f(x) = 0 \cdot x$

$f(x + y) = 0 \cdot (x + y) = 0 \cdot x + 0 \cdot y$

$= f(x) + f(y),\ \forall x, y \in Z_4$

Yes.

Theorem: A mapping $f : G \to G'$ is homomorphism then

(i) $f(e) = e',\ \ e' \in G'$

(ii) $f(x^{-1}) = [f(x)]^{-1}$

Proof:

(i) Let $f : G \to G'$ is a homomorphism and $e \in G$ also $e' \in G'$

$f(x) \cdot e' = f(x)$

$= f(x \cdot e)$

$= f(x) \cdot f(e)$

then $f^{-1}(x)$ exists

$\Rightarrow f^{-1}(x) f(x) \cdot e' = f^{-1}(x) \cdot f(x) \cdot f(0)$

$e \cdot e' = e \cdot f(e)$

$\therefore f(e) = e'$

(ii) $f(x^{-1}) = [f(x)]^{-1}$

$x \in G$ then $xx^{-1} = e$

$f(xx^{-1}) = f(e)$

$\Rightarrow f(x) \cdot f(x^{-1}) = e'$

$\Rightarrow f(x^{-1}) = [f(x)]^{-1} e'$

$\Rightarrow f(x^{-1}) = [f(x)]^{-1}$

Kernel of Homomorphism

A mapping $f : G \to G'$ is homomorphism then kernel of homomorphism is defined by

$\ker f = \{x \in G \mid f(x) = e', e' \in G'\}$

Theorem: Show that

A mapping $f: G \to G'$ is homomorphism then ker f is subgroup of G.

$\ker f = \{x \in G \mid f(x) = e'\}$

Let $x \in \ker f \Rightarrow f(x) = e'$ ....(1)

$y \in \ker f \Rightarrow f(y) = e'$ ....(2)

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

$= f(x) \cdot [f(y)]^{-1}$ [$f(y^{-1}) = [f(y)]^{-1}$, $\because f$ is homomorphism]

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

$= e' \cdot e'$

$= e'$

$f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \ker f$

Hence, $\ker f$ is subgroup of G.

Q. Show that $\ker f = \{x \in G \mid f(x) = e'\}$ is homomorphism where mapping is $f: G \to G'$ then this is normal subgroup of G.

Solution:

$f: G \to G'$ is homomorphism and $x \in G, h \in \ker f\ f(h) = e'$

then $f(xhx^{-1}) = f(x) f(h) f(x^{-1})$

$= f(x) \cdot e' \cdot f(x^{-1})$

$= f(x) \cdot [f(x)]^{-1}$

$= e'$

$f(xhx^{-1}) = e' \Rightarrow xhx^{-1} \in \ker f$

then $\ker f$ is normal subgroup of G.

Image of Homomorphism

A mapping $f: G \to G'$ is homomorphism then $\operatorname{Im} f = \{f(x) \mid x \in G\}$

Q. Show that Im *f* is subgroup of G'.

Solution:

Let $f(x) \in \operatorname{Im} f$, $x \in G$

$f(y) \in \operatorname{Im} f$, $y \in G$

$f(x)[f(y)]^{-1} = f(x) \cdot f(y^{-1})$

$= f(xy^{-1})$ [$\because$ homogeneous]

$x \in G \Rightarrow xy^{-1} \in G$ because G is group then $f(xy^{-1}) \in \operatorname{Im} f$

$\Rightarrow f(x) \cdot [f(y)]^{-1} \in \operatorname{Im} f$

Then $\operatorname{Im} f$ is subgroup of G'.

Onto-homomorphism: A mapping $f : G \to G'$ is said to be onto homomorphism if
(i) *f* is homomorphism
(ii) *f* is onto

Exam Point-: $f : Z_m \to Z_n,\ f(x) = ax,\ a \in Z_n$. First find $O(a)$ in Z_n, suppose $O(a) = k$ in Z_n and Z_m has elements of order k then $f(x) = ax$ is homomorphism.

Exam Point:
: Let $f : Z_m \to Z_n$
Number of such group homomorphisms $= \gcd(m,n)$

Q. $f : Z_4 \to Z_{10}$ defined by $f(x) = 1\cdot x$ is homomorphism.
Solution: No
$f : Z_4 \to Z_{10}$
Let $x = 3, y = 1,\ x \in Z_4, y \in Z_4$
$f(3+1) = f(4) = f(0) = 1\cdot 0 = 0$
$f(3) + f(1) = 1\cdot 3 + 1\cdot 1 = 4$
$f(x+y) \neq f(x) + f(y)$ i.e. $0 \neq 4$
$\therefore f(x) = 1\cdot x$ is not homomorphism.
Q. $f : Z_4 \to Z_{10}$ defined by $f(x) = 2x$ is a homomorphism?
Solution:
$f(x) = 2x$
$x = 3, y = 1,\quad x \in Z_4, y \in Z_4$
$f(3+1) = f(4) = f(0) = 0$
$f(3) + f(1) = 2\cdot 3 + 2\cdot 1 = 8$
$0 \neq 8$
$f(3+1) \neq f(3) + f(1)$
$f(x) = 2x$ is not a homomorphism.
Q. $f : Z_4 \to Z_{10}$ how many group homomorphism?
$f(x) = 0\cdot x\,\surd,\ f(x) = 1\cdot x\times,\ f(x) = 2\cdot x\times$
$f(x) = 3\cdot x\times,\ f(x) = 4\cdot x\times, f(x) = 5\cdot x\,\surd$
$f(x) = 6\cdot x\times, f(x) = 7\cdot x\times, f(x) = 8\cdot x\times$
$f(x) = 9\cdot x\times,$
So $f(x) = 0\cdot x$ and $f(x) = 5\cdot x$ are group homomorphism.
Exactly 2 group homomorphism.

Q. $f: Z_5 \to Z_{10}$ how many group homomorphism?

Solution:

$f(x) = 0 \cdot x \surd,\ f(x) = 1 \cdot x \times$

$f(x) = 2 \cdot x \surd,\ f(x) = 3 \cdot x \times,\ f(x) = 4 \cdot x \surd,\ f(x) = 5 \cdot x \times,\ f(x) = 6 \cdot x \surd,\ f(x) = 7 \cdot x \times$

$f(x) = 8 \cdot x \surd,\ f(x) = 9 \cdot x\ \times$

Q. $f: Z_3 \to Z_9$, how many group homomorphism?

Solution:

$f: Z_3 \to Z_9$

$f(x) = 0 \cdot x \surd,\ f(x) = 1 \cdot x \times,\ f(x) = 2 \cdot x \times,\ f(x) = 3 \cdot x \surd$

$f(x) = 4 \cdot x \times,\ f(x) = 5 \cdot x \times,\ f(x) = 6 \cdot x \surd,\ f(x) = 7 \cdot x \times,\ f(x) = 8 \cdot x \times$

$f(x) = 0 \cdot x, 3 \cdot x, 6x$ are group homomorphisms.

3 group homeomorphisms are there.

Q. $f: Z_6 \to Z_6$, how many homeomorphisms

Solution:

$\gcd(6,6) = 6$

6-group homomorphisms they are

$f(x) = 0 \cdot x, 1 \cdot x, 2 \cdot x, 3 \cdot x, 4 \cdot x, 5 \cdot x$

Checking:

$f(5+1) = f(6) = f(0) = 0$

$f(5) + f(1) = 1 \cdot 5 + 1 \cdot 1 = 6 = 0$

$f(5+1) = f(5) + f(1)$

$\therefore f(x) = 1 \cdot x$ is homomorphism.

Q. How many homeomorphisms $f: Z_4 \to Z_8$?

Solution:

Possible orders of elements in Z_8 are 1,2,4,8

Possible order of elements in Z_4 are 1,2,4

Common order of elements in Z_4 and Z_8 are 1,2 and 4.

Number of elements of order 1 in $Z_8 = \phi(1) = 1$

Number of elements of order 2 in $Z_8 = \phi(2) = 1$

Number of elements of order 4 in $Z_8 = \phi(4) = 2$

Total = 4

Total No. of Homeomorphisms = 1+1+2 = 4

i.e. Total No. of common elements in Z_8 = No. of homeomorphisms

$f: Z_4 \to Z_8$

$f(x) = 0 \cdot x \to$ order $\to 1$

$f(x) = 4 \cdot x \to$ order $\to 2$

$f(x) = 2 \cdot x \rightarrow$ order $\rightarrow 4$

$f(x) = 6 \cdot x \rightarrow$ order $\rightarrow 4$

Q. $f : Z_{12} \rightarrow Z_4$, how many homeomorphisms.

Solution: No. of homomorphism = gcd (12,4) - 4

Possible order of elements in $Z_4 = 1, 2$ and 4

Possible order of elements in $Z_{12} = 1, 2, 4, 6, 12$

Common order of elements in Z_{12} and $Z_4 = 1, 2$ and 4

Number of elements of order 1 in $Z_4 = \phi(1) = 1$

Number of elements of order 2 in $Z_4 = \phi(2) = 1$

Number of elements of order 4 in $Z_4 = \phi(4) = 2$

Total No. of homeomorphisms $= 1 + 1 + 2 = 4$

$f : Z_{12} \rightarrow Z_4, \quad f(x) = ax, a \in Z_4$

$f(x) = 0 \cdot x$ √ order (0) = 1

$f(x) = 1 \cdot x$ √ order (1) = 4

$f(x) = 2 \cdot x$ √ order (2) = 2

$f(x) = 3 \cdot x$ √ order (3) = 4

Q. How many homomorphism in $f : Z_8 \rightarrow Z_2 \times Z_4$.

Solution:

Possible order of elements in $Z_8 = 1, 2, 4$ and 8

Possible order of elements in $Z_2 \times Z_4 = 1, 2, 4$

Common order of elements in Z_8 and $Z_2 \times Z_4$ are $= 1, 2, 4$

# of elements of order 1 in $Z_2 \times Z_4 = \phi(1) \cdot \phi(1) = 1$

# of elements of order 2 in $Z_2 \times Z_4$

$2 \quad 1 = \phi(2) \cdot \phi(1) = 1$

$1 \quad 2 = \phi(2) \cdot \phi(1) = 1$

$2 \quad 2 = \phi(2) \cdot \phi(2) = 1 + 1 = 1$

of order 4 in $Z_2 \times Z_4$

$1 \quad 4 = \phi(1) \cdot \phi(4) = 2$

$2 \quad 4 = \phi(2) \cdot \phi(4) = 2$

Total = 4

Total No. of homeomorphisms $= 1 + 3 + 4 = 8$

Exam Point-: Number of Homomorphisms from $f : Z_m \times Z_n \rightarrow Z_k = \gcd(m, k) \times \gcd(n, k)$

Exam Point-: $f : Z_m \times Z_n \rightarrow Z_k \times Z_l$

No. of homomorphisms = $\gcd(m, k) \times \gcd(m, l) \times \gcd(n, k) \times \gcd(n, l)$

Exam Point: Number of Homomorphisms from $f : Z_m \rightarrow Z_n \times Z_k$

$= \gcd(m,n) \times \gcd(m,k)$

Examples

$f : Z_8 \to Z_2 \times Z_4$

$f(x) = (a,b)\cdot x,\ (a,b) \in Z_2 \times Z_4$

$f(x) = (0,0)\cdot x$ order $\to 1$

$f(x) = (1,0)\cdot x$ order $\to 2$

$f(x) = (0,2)\cdot x$ order $\to 2$

$f(x) = (1,2)\cdot x$ order $\to 2$

$$\left.\begin{aligned} f(x) &= (0,1)\cdot x \\ f(x) &= (0,3)\cdot x \\ f(x) &= (1,1)\cdot x \\ f(x) &= (1,3)\cdot x \end{aligned}\right\} \text{order} \to 4$$

Q. How many homomorphism from

$f : Z_2 \times Z_4 \to Z_8$?

Solution:

Possible order or elements in Z_2 are 1,2

Possible order of elements in Z_4 are 1,2 and 4

Possible order of elements in Z_8 are 1,2,4,8

Common order of elements in Z_2 and Z_8 are 1,2

Number of elements order 1 in $Z_8 = \phi(1) = 1$

Number of elements order 2 in $Z_8 = \phi(2) = 1$

Total No. of homeomorphisms from Z_2 to Z_8

$= 1 + 1 = 2$ ....(1)

Common order of elements in Z_4 and Z_8 are 1,2,4

Number of elements or order 1 in $Z_8 = \phi(1) = 1$

Number of elements order 2 in $Z_8 = \phi(2) = 1$

Number of elements order 4 in $Z_8 = \phi(4) = 2$

Total = 4

Total homomorphism from Z_4 to $Z_8 = 1 + 1 + 2 = 4$ ....(2)

$\therefore$ Total homomorphism from $Z_2 \times Z_4$ to Z_8 $= 2 \times 4 = 8$

Q. $f : Z_2 \times Z_4 \to Z_2 \times Z_4$

Solution:

$2\times2\times2\times4=32$

Q. $f:Z\to Z, f(x)=0\cdot x$ is homomorphism

Solution:

$f(x)=0\cdot x$

$f(x+y)=0\cdot(x+y)=0\cdot x+0\cdot y=f(x)+f(y)$ then $f(x)=0\cdot x$ is homomorphism.

Now, $f(x)=1\cdot x$

then $x,y\in Z$

$f(x+y)=1\cdot(x+y)=1\cdot x+1\cdot y=f(x)+f(y), \quad \forall x,y\in Z$ then $f(x)=1\cdot x$ is homomorphism.

Q. $f:Z\to Z, \quad f(x)=kx$ is a homomorphism?

Solution: $f(x+y)=k(x+y)=k\cdot x+k\cdot y=f(x)+f(y)$

then $f(x)=kx$ is a homomorphism.

Exam Point-: Infinite Number of homomorphisms from Z to Z.

Que. $f:Z_8\to Z_4, \; f(x)=1\cdot x$ is onto homomorphism.

Solution:

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

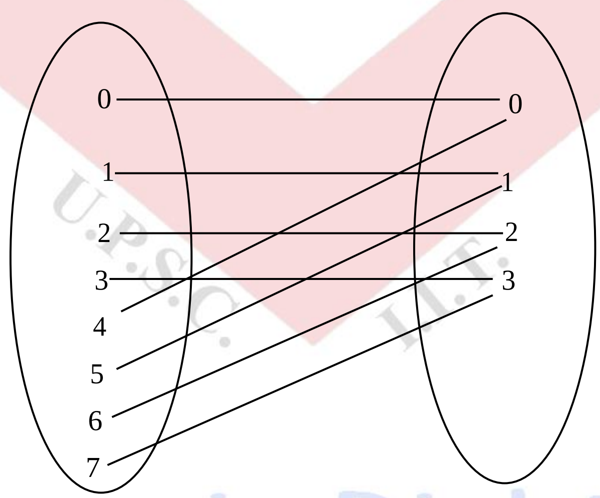
$Z_4=\{0,1,2,3\}$

$f(x)=x$, $f(0)=0$, $f(1)=1$, $f(2)=2$, $f(3)=3$

$f(4)=0$, $f(5)=1$, $f(6)=2$, $f(7)=3$

$\operatorname{Im} f=\{0,1,2,3\}\approx Z_4$

$\therefore f(x)=x$ is onto.



$f:Z_8\to Z_4$

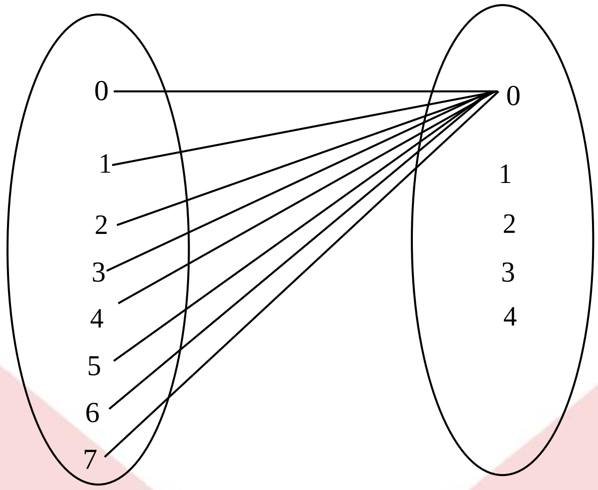
$f(x)=x$ is onto homomorphism.

Q. $f:Z_8\to Z_4, \; f(x)=0\cdot x$ is onto homomorphism?

Solution:

$f(x)=0, \quad \forall x \in Z_8$

then $f(x)$ is not onto.



Q. $f: Z_8 \to Z_4, f(x)=2\cdot x$ is onto homomorphism?

Solution:

$f(x)=2x$

$f(0)=0$, $f(1)=2$, $f(2)=0$, $f(3)=2$, $f(5)=2$, $f(6)=0$, $f(7)=2$

$\operatorname{Im} f=\{0,2\} \not\approx Z_4$

then $f(x)=2x$ is not onto homomorphism?

Q. $f: Z_8 \to Z_3, f(x)=1\cdot x$ is this onto homomorphism?

Solution:

Mapping is not a homomorphism hence it is not an onto homomorphism.

$1\in Z_3$ and $O(1)$ in Z_3 is 3 but Z_8 has no element of order 3 then $f(x)=1\cdot x$ is not homomorphism

then $f(x)=1\cdot x$ is not onto homomorphism.

Exam Point-7: $f: Z_m \to Z_n$, $n\,|\,m$ # of onto homomorphism $=\phi(n)$.

Q. $f: Z_{10} \to Z_4$ has onto homomorphism?

Solution:

No. of homomorphism from Z_{10} to Z_4

$=\gcd(10,4)=2$

i.e. $f(x)=0\cdot x$ and $f(x)=2\cdot x$

but neither $f(x)=0\cdot x$ nor $f(x)=2\cdot x$ is onto mapping.

Q. $f: Z_{10} \to Z_5$, how many onto homomorphism?

Solution:

No. of homomorphism from Z_{10} to Z_5

$=\gcd(10,5)=5$

they are

$$\left.\begin{aligned} f(x) &= 0\cdot x \\ f(x) &= 1\cdot x \\ f(x) &= 2\cdot x \\ f(x) &= 3\cdot x \\ f(x) &= 4\cdot x \end{aligned}\right\}\text{ homomorphism}$$

here

$$\left.\begin{aligned} f(x) &= 1\cdot x \\ f(x) &= 2\cdot x \\ f(x) &= 3\cdot x \\ f(x) &= 4\cdot x \end{aligned}\right\}\text{ onto homomorphism.}$$

Q. $f : Z_{20} \to Z_{10}$, how many onto homomorphism

Solution:

10|20, then no. of onto homomorphism $= \phi(10) = 4$

$$\left.\begin{aligned} f(x) &= 1\cdot x \\ f(x) &= 3\cdot x \\ f(x) &= 7\cdot x \\ f(x) &= 9\cdot x \end{aligned}\right\}\text{ onto homomorphism}$$

Q. $f : Z \to Z$, how many onto homomorphism?

Solution:

$$\left.\begin{aligned} f(x) &= 1\cdot x \\ f(x) &= -1\cdot x \end{aligned}\right\}\text{ onto homomorphism}$$

exactly two onto homomorphism.

Isomorphism

A mapping $f : G \to G'$ is said to be isomorphism if

(i) *f* is homomorphism

(ii) *f* is one-one

(iii) *f* is onto

Q. $f : Z \to Z$, $f(x) = 1\cdot x$ is isomorphism?

Solution:

f is homomorphism, one-one and onto then *f* is isomorphism.

Similarly

$f : Z \to Z = -x$ is also, homomorphism, one-one and onto then $f(x) = -x$ is isomorphism.

Q. $f : Z_{15} \to Z_{15}$, $f(x) = 1\cdot x$ is isomorphism?

Solution:

$f(x) = 1\cdot x,\ O(1)$ in $Z_{15} = 15,\ Z_{15}$ (LHS)

has element of order 15 then $f(x) = 1\cdot x$ is homomorphism.

***f* is one-one**:
$f(x_1) = f(x_2), \quad x_1, x_2 \in Z_{15}$ (LHS)
$\Rightarrow x_1 = x_2$
f is one-one.
***f* is onto**: $O(Z_{15}(\text{LHS})) = O(Z_{15}(\text{RHS})) = 15$ and *f* is one-one then *f* is onto.

Q. $f : Z_{20} \to Z_{20}$, how many isomorphism?
Solution:
20|20, then no. of onto homomorphism
$= \phi(20) = 8$ = one-one homomorphism
(cardinality of domain and co-domain are same).
and they are:

$$\left.\begin{array}{l} f(x) = 1 \cdot x \\ f(x) = 3 \cdot x \\ f(x) = 7 \cdot x \\ f(x) = 9 \cdot x \\ f(x) = 11 \cdot x \\ f(x) = 13 \cdot x \\ f(x) = 17 \cdot x \\ f(x) = 19 \cdot x \end{array}\right\} \text{isomorphism in } f : Z_{20} \to Z_{20}$$

Properties of Isomorphism

Suppose that ϕ is an isomorphism from a group G onto a group $\bar{G}$. Then
(i) ϕ carries the identity of G to the identity of $\bar{G}$
(ii) For every integer *n* and for every group element *a* in G, $\phi(a^n) = [\phi(a)]^n$
(iii) For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
(iv) G is abelian if and only if $\bar{G}$ is abelian.
(v) $|a| = |\phi(a)|$ for all a in G. (Isomorphism preserves orders)
(vi) G is cyclic if and only if $\bar{G}$ is cyclic.
(vii) For a fixed integer *k* and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\bar{G}$.
(viii) ϕ^{-1} is an isomorphism from $\bar{G}$ onto G.
(ix) If *k* is a subgroup of G, then $\phi(k) = \{\phi(k) : k \in K\}$ is a subgroup of $\bar{G}$.

Exam Point: Proofs are easy to do and also if you do those, you'll feel these properties. But in exam; proofs of these properties are not expected to ask. So you can just read about proofs (either from classnotes or book (galian P. 123).
You need to remember these properties, those will help you in solving other questions.

[1] Cayley's theorem: (The same logic as in the previous proof, we applied): For details check the lecture as well.

[2] A finite cyclic group is isomorphic of $\mathbf{Z}_n$ where of order of that group is *n*.

AUTOMORPHISM

A mapping $f : G \to G$ is said to be automorphism if

(1) *f* is homomorphism
(2) f is one-one
(3) *f* is onto

Q. $f : Z_{15} \to Z_{15}$, find number of automorphism?

Solution:

$f : Z_{15} \to Z_{15}$

$$\left.\begin{array}{l} f_1(x) = 1 \cdot x \\ f_2(x) = 2 \cdot x \\ f_3(x) = 4 \cdot x \\ f_4(x) = 7x \\ f_5(x) = 8x \\ f_6(x) = 11x \\ f_7(x) = 13x \\ f_8(x) = 14x \end{array}\right\}$$ There are homomorphisms, one-one and onto. Then, automorphism also.

Then, exactly 8 automorphism from Z_{15} to Z_{15}.

NOTE: $f : Z_m \to Z_m$ has exactly $\phi(n)$ automorphism.

Q. $f : Z \to Z$, how many automorphism?

Solution:

$f : Z \to Z$

$f(x) = 1x$

$f(x) = -1x$

homomorphism, one-one and onto then $f(x) = x$ and $f(x) = -x$ are automorphism.

Exactly 2 automorphisms from Z to Z.

Q. $f : Z \to Z$, $f_1(x) = 1x$ and $f_2(x) = -1x$

Aut(z) = {Set of all automorphsim of Z} and Aut (z) $\approx$?

Solution:

$f : Z \to Z$

$$\left.\begin{aligned} f_1(x) &= 1x \\ f_2(x) &= -1x \end{aligned}\right\}\text{Automorphism}$$

$\text{Aut}(z) = \{1x, -1x\} = \{f_1, f_2\}$

Now we to check that is $\text{Aut}(z)$ is a group wrt composition or not.

(1) Closure Property:

$(f_2 f_2)(x) = f_2(f_2(x))$

$= f_2(-x)$

$= x = f(x)$

	f_1	f_2
f_1	f_1	f_2
f_2	f_2	f_1

Closure satisfied

$a \in \text{Aut}(z), b \in \text{Aut}(z)$

$ab \in \text{Aut}(z)$

$ab \in \text{Aut}(z)$

$(f_1 f_1)(x)$

$= f_1(f_1(x))$

$= f_1(x)$

$= x$

$= f_1$

$(f_1 f_2)(x) =$

$= f_1(f_2(x))$

$= f_1(-x)$

(2) **Associative -** Mapping composition always satisfied associative property.

(3) **Identity -** $\forall f \in \text{Aut}(z) \Rightarrow f_1 \in \text{Aut}(z)$

f_1 is identity from composition table

$f \circ f_1 - f_1 \circ f = f$

(4) Inverse: $\forall f \in \text{Aut}(z), \exists f^{-1} \in \text{Aut}(z)$

s.t. $f^{-1} \circ f^{-1} = f^{-1} \circ f = I$

$f_1^{-1} = f_1$ and $f_2^{-1} = f_2$

then $\text{Aut}(z)$ is group wrt composition and $O(\text{Aut}(z)) = 2 \approx Z_2$

$f_2 \in \text{Aut}$ s.t. $O(f_2) = 2 = 0(\text{Aut}(z))$ then $\text{Aut}(z) \approx z_2$

Q. Find $\text{Aut}(z_{10})$ = ?

Solution:

$f : Z_{10} \to Z_{10}$

$$\left.\begin{aligned} f_1(x) &= 1x \\ f_2(x) &= 3x \\ f_3(x) &= 7x \\ f_4(x) &= 9x \end{aligned}\right\} \text{There are automorphisms}$$

$\text{Aut}(Z_{10})$ = {Set of all automorphism from Z_{10} to Z_{10} }

Aut $(Z_{10}) = \{x, 3x, 7x, 9x\} = \{f_1, f_2, f_3, f_4\}$

$O(\text{Aut}(Z_{10})) = 4$

Aut (Z_{10}) is group w.r.t. composition

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_4	f_1	f_3
f_3	f_3	f_4	f_1	f_3
f_4				

$(f_1 f_1)(x) = f_1(f_1(x))$

$= f_1(x) = x$

$= f_1$

$(f_1 f_2)(x) = f_1(f_2(x))$

$= f_1(3x)$

$= f_2$

$(f_2 f_2)(x) = f_2(f_2(x))$

$= f_2(3x) = 3(3x)$

$= 9x = f_4$

$(f_2 f_3)(x) = f_2(f_3(x))$

$= f_2(7x)$

$= 3 \cdot 7x = 21x$

$= x = f_1$

From Composition table $\text{Aut}(Z_{10})$ is group with identity $f_1(x) = x$ and

$f_1^{-1} = f_1, f_2^{-1} = f_3, f_3^{-1} = f_2, f_4^{-1} = f_4$

$O(\text{Aut}(Z_{10})) = 4$

$f_2 \in \text{Aut}(Z_{10})$ s.t. $O(f_2) = 4 = O(\text{Aut}(Z_{10}))$

$\Rightarrow (\text{Aut}(Z_{10}))$ is cyclic so $\text{Aut}(Z_{10}) \approx Z_4$

$(f_2)^4 = I$

$(f_2 \cdot f_2)(x) = f_4(x)$

$(f_2 \cdot f_2 \cdot f_2 \cdot f_2)(x) = (f_4 \cdot f_4)(x)$

$= f_1(x)$

$(f_2)^4 = f_1 = I$

$\Rightarrow O(f_2) = 4$

NOTE: Set of all automorphism of G form a group w.r.t composition it is denoted by $\text{Aut}(G)$.

Q. (i) Find $\text{Aut}(Z_{20}) \approx ?$

(ii) Find Aut $(Z_8) \approx ?$

Solution:

(ii) $f : Z_8 \to Z_8$

$$\left.\begin{array}{l} f_1(x) = 1x \\ f_2(x) = 3x \\ f_3(x) = 5x \\ f_4(x) = 7x \end{array}\right\} \text{There are automorphism}$$

$\text{Aut}(Z_8) = \{x, 3x, 5x, 7x\} = \{f_1, f_2, f_3, f_4\}$

$O(\text{Aut}(Z_8)) = 4$

$$O(\text{Aut}(Z_8)) = 4 \begin{cases} Z_4 \\ Z_2 \times Z_2 \end{cases}$$

$O(f_1) = 1,\ O(f_3) = 2$

$O(f_2) = 2,\ O(f_4) = 2$

then

$\text{Aut}(Z_8) \approx Z_2 \times Z_2$

(i) $\text{Aut}(Z_{40}) \approx Z_2 \times Z_2 \times Z_4$

$U(8 \times 5) = U(8) \times U(5)$

$= U(2^3) \times U(5)$

$\approx Z_2 \times Z_2 \times Z_4$

Note: $\text{Aut}(Z_n) \approx U(n)$

Q. Find $\text{Aut}(Z_{20}) = ?$

Solution:

$f : Z_{20} \to Z_{20}$

$f_1(x) = 1x$

$f_2(x) = 3x$
$f_3(x) = 7x$
$f_4(x) = 9x$
$f_5(x) = 11x$
$f_6(x) = 13x$
$f_7(x) = 17x$
$f_8(x) = 19x$
Aut $(Z_{20}) = \{x, 3x, 7x, 9x, 11x, 13x, 17x, 19x\}$
$= \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$
$O(\text{Aut}(Z_{20})) = 8$
$f_5 \in \text{Aut}(Z_{20})$ s.t.
$O(f_5) = 2$

$$f_5(x) = 11x$$
$$(f_5 \cdot f_5)(x) = 11 \cdot 11x$$
$$= 121x$$
$$= x = f_1(1)$$

Similarly, $f_8(x) \in \text{Aut}(Z_{20})$ s.t. $O(f_8) = 2$
$(f_8 \cdot f_8)(x) = f_8(f_8(x))$
$= 19 \cdot 19x = 361x$
$= x = f_1(x)$
$\Rightarrow \text{Aut}(Z_{20}) \not\approx Z_8$
because Z_8 has exactly one element of order 2 but Aut (Z_{20}) has more than one element of order 2.
Now,
$f_3 \in \text{Aut}(Z_{20})$ s.t. $O(f_3) = 4$
then $\text{Aut}(Z_{20}) \not\approx Z_2 \times Z_2 \times Z_2$ because $Z_2 \times Z_2 \times Z_2$ has no elements of order more than 2.
Then,
$\text{Aut}(Z_{20}) \approx Z_2 \times Z_4$

Q. How many elements of order 2 in $\text{Aut}(Z_{21})$?
Solution:
$f : Z_{21} \to Z_{21}$
$\text{Aut}(Z_{21}) = \{x, 2x, 4x, 5x, 8x, 10x, 11x, 13x, 16x, 17x, 19x, 20x\}$
$= \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}, f_{12}\}$
$\text{Aut}(Z_{21}) \approx U(21) = U(7 \times 3) \approx U(7) \times U(3)$
$\approx Z_6 \times Z_2$

$2\ 1 = \phi(2)\cdot\phi(1) = 1$

$1\ 2 = \phi(1)\cdot\phi(1)\cdot\phi(2) = 1$

$2\ 2 = \phi(2)\cdot\phi(3) = 1$

Then, exactly 3 elements or order 2 in $\text{Aut}(Z_{21})$

Q. $\text{Aut}(Z_n)$ is always cyclic?

i.e. If G be a finite cyclic group of order *n* then $\text{Aut}(G)$ is always cyclic.

Solution:

Need not be $G = Z_{12}$ is cyclic group or order 12

$\text{Aut}(G)$ = $\text{Aut}(Z_{12}) \approx U(12) \approx Z_2 \times Z_2$

then $\text{Aut}(Z_{12}) \approx Z_2 \times Z_2$ and $Z_2 \times Z_2$ is not cyclic then $\text{Aut}(Z_n)$ is not always cyclic.

NOTE: $\text{Aut}(Z_n)$ is always abelian As $\text{Aut}(Z_n) \approx U(n)$, since $U(n)$ is always abelian so $\text{Aut}(Z_n)$ is always abelian.

Q. If $\text{Aut}(G_1) \approx \text{Aut}(G_2) \Rightarrow G_1 \approx G_2$?

Solution:

$G_1 = Z_{10}$ and $G_2 = Z_5$

$\text{Aut}(Z_{10}) \approx U(10)$ Aut $(Z_5) \approx U(5)$

$\Rightarrow \text{Aut}(Z_{10}) \approx Z_4$ and $\text{Aut}(Z_5) \approx Z_4$

$\text{Aut}(Z_{10}) \approx Z_4 \approx \text{Aut}(Z_5)$

but $Z_{10} \not\approx Z_5$

$\therefore \text{Aut}(G_1) \approx \text{Aut}(G_2)$ then $G_1 \approx G_2$ is need not be true.

NOTE: (i) No. of Automorphism in $S_n = n!, n \geq 3$

(ii) No. of Automorphism in $D_n = n\phi(n), n \geq 3$

NOTE:

$f : Z_p \times Z_p \times Z_p, \ldots . Z_p \to Z_p \times Z_p \times \ldots . \times Z_p$

$\text{Aut}(Z_p \times Z_p \times \ldots . \times Z_p) \approx GL_n(Z_p)$.

$\boxed{\text{Aut}(Z_n) \approx U(n)}$.

Let's learn; how to visualize theory proofs with the help of examples (my own experience).

Example: Let's think about $\mathbf{Z}_{10}$

Step (i): Definition of Aut (G): An isomorphism from a group G onto itself is called an automorphism of G collection of all such automorphisms of G is represented by Aug(G).

Example to visualize definition:

Let $\alpha \in \text{Aut}(Z_{10})$; now let's try to discover enough information about α to determine how α must be defined.

Let's begin with $\alpha(1) =$ __________ ?

$\therefore \alpha$ is an isomorphism from $\mathbf{Z}_{10}$ to $\mathbf{Z}_{10}$

$\therefore |\alpha(1)| = |1|$ in $\mathbf{Z}_{10} = 10$

$\therefore$ There are four choices for $\alpha(1)$:

$\alpha(1) = 1 = \alpha_1$ (say)

$\alpha(1) = 3 = \alpha_3$ (say)

$\alpha(1) = 7 = \alpha_7$ (say)

$\alpha(1) = 9 = \alpha_9$ (say)

Let's write $\text{Aut}(\mathbf{Z}_{10}) = \{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$

for composition, we may observe α_1 working as identity,

$(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$

$\therefore \alpha_3\alpha_3 = \alpha_9, \quad \alpha_3^4 = \alpha_1, \therefore |\alpha_3| = 4$

Aut (Z_{10})

$\text{Aut}(Z_{10})$	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

U(10)

$U(N)$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Actual Proof:

With the above example, now we are ready to tackle the group Aut (Z_n):

$\because$ Any automorphism α is determined by the value of $\alpha(1)$ and $\alpha(1) \in U(n)$.

Now consider the correspondence from Aut (Z_n) to $U(n)$ given by $T : \alpha \to \alpha(1)$.

Aut (Z_n) to $U(n)$ given by $T : \alpha \to \alpha(1)$.

The fact that $\alpha(k) = k\alpha(1)$ implies

T is one-one mapping.

- To prove T is onto:

Let $r \in U(n)$ and consider the mapping α from $\mathbf{Z}_n$ to $\mathbf{Z}_n$ defined by $\alpha(s) = sr(\bmod n)$ for all *s* in $\mathbf{Z}_n$ (Also α is an automorphism) then,

$\because T(\alpha) = \alpha(1) = r$, T is onto $U(n)$.

- T is operator preserving:

Let $\alpha, \beta \in \text{Aut}(Z_n)$

$T(\alpha\beta) = (\alpha\beta)(1) = \alpha(1+1+1+....+1)$ β-times $= \beta(1)$

$= \alpha(1) + \alpha(1) + ... + \alpha(1)$

$= \alpha(1)\beta(1) = T(\alpha)T(\beta)$

This completes the proof.

INNER AUTOMORPHISM

Let $a \in G$ the mapping $Ta : G \to G$ defined by $T_a(x) = axa^{-1}$ is Inner Automnorphism if

(i) T_a is homomorphism

(ii) T_a is one-one

(iii) T_a is onto

Verification of Definition:

$a \in G, T_a : G \to G$ defined by $T_a(x) = axa^{-1}$ is

(i) T_a is homorphism

(ii) T_a is one-one

(iii) T_a is onto

Proof:

$T_a : G \to G*$

$T_a(x) = axa^{-1}$

(i) T_a is homomorphism: Let $x, y \in G$

$T_a(x, y) = a(xy)a^{-1}$

$= axeya^{-1} \; ; aa^{-1} = e$

$= axa^{-1}aya^{-1}$

$\therefore T_a(xy) = (axa^{-1})(aya^{-1})$

$\therefore T_a(xy) = T_a(x) \cdot T_a(y)$

T_a is homomorphism.

(ii) and (iii) T_a is one-one and onto

$T_a(x) = axa^{-1}, \; a \in G$, since G is group then $\exists$ unique $a^{-1} \in G$ s.t.

$T_{a^{-1}}(x) = a^{-1}x(a^{-1})^{-1}$

$= a^{-1}xa$

Now, we will show that $T_{a^{-1}}$ is inverse of T_a

$(T_a T_{a^{-1}})(x) = T_a(T_{a^{-1}}(x))$

$= T_a(a^{-1}xa)$

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

$= (aa^{-1})x(aa^{-1})$

$= exe$

$= exe^{-1}$

$= T_e(x)$

$\Rightarrow T_a T_{a^{-1}} = T_e$

then $(Ta)^{-1} = T_{a^{-1}}$

NOTE: Set of all Inner Automorphism of G form a group wrt comparisiton, it is denoted by

$$I_{nn}(G) = \{T_a | a \in G\} \approx \frac{G}{Z(G)}$$

Q. How many Inner Automotphsim in Z_{10}?

Solution:

$G = Z_{10}$

$$I_{nn}(G) = \frac{G}{Z(G)}$$

$$O(I_{nn}(G)) = \frac{O(G)}{O(Z(G))} = \frac{O(Z_{10})}{O(Z(Z_{10}))} = \frac{10}{10} = 1$$

$T_a = axa^{-1} = aa^{-1}x = e \cdot x = x$ (G is abelian $xa^{-1} = a^{-1}x$)

Q. How many Inner Automorphism in S_3?

Solution:

$$I_{nn}(S_3) = \frac{S_3}{Z(S_3)}$$

$$O(I_{nn}(S_3)) = \frac{O(S_3)}{O(Z(S_3))} = \frac{6}{1} = 6$$

Q. How many Inner Automorphism in D_3?

Solution:

$$I_{nn}(D_3) = \frac{D_3}{Z(D_3)}$$

$$O(I_{nn}(D_3)) = \frac{O(D_3)}{O(Z(D_3))} = \frac{6}{1} = 6$$

Q. $I_{nn}(G) = \{e\}$ iff G is abelian.

Solution:

Let G be abelian then

$\Rightarrow Z(G) = G$

$$I_{nn}(G) \approx \frac{G}{Z(G)} \approx \frac{G}{G} \approx Z_1$$

$\frac{G}{Z(G)} \approx Z_1$, Z_1 is cyclic then $G = \{e\}$

$$I_{nn}(G) = \frac{G}{Z(G)} \approx Z_1 \approx \{e\}$$

Conversely, $I_{nn}(G) = \{e\}$

$$\Rightarrow \frac{G}{Z(G)} \approx Z_1$$

Since Z_1 is cyclic then G is abelian.

NOTE: If G is abelian then $I_{nn}(G) \approx Z_1$ No. Inner automorphism is 1.

Q. $G = A_3 \times D_4 \times S_3 \times Z_4$, find no of inner automorphism.

Solution:

$$G = A_3 \times D_4 \times S_3 \times Z_4$$

$$I_{nn}(G) \approx \frac{G}{Z(G)}$$

$$O(I_{nn}(G)) = \frac{O(G)}{O(Z(G))} = \frac{3 \times 8 \times \cancel{6} \times \cancel{4}}{\cancel{3 \times 2} \times 1 \times \cancel{4}} = 24$$

Q. $G = Z, G = Q, G = \mathbf{R}, G = \mathbf{C}, G = \mathbf{R} \times \mathbf{R}$

$$G = Z \times Q \times \mathbf{R} \times \mathbf{C} \approx Z_1$$

$$I_{nn}(Z) = I_{nn}(\mathbf{R}) = I_{nn}(\mathbf{C}) = I_{nn}(\mathbf{R} \times \mathbf{R}) \approx Z_1$$

Q. Find no of Inner Automorphism in Q_4?

Solution:

Inner Automorphism of Q_4

$$I_{nn}(Q_4) \approx \frac{Q_4}{Z(Q_4)}$$

$$O(I_{nn}(Q_4)) = O\left(\frac{Q_4}{Z(Q_4)}\right) = \frac{O(Q_4)}{O(Z(Q_4))} = \frac{8}{2} = 4$$

Then Q_4 has exactly 4 inner automorphism.

Q. Find number of inner automorphism in $D_n, n \geq 3$?

Solution:

Case I: If n is odd then

$$I_{nn}(D_n) \approx \frac{D_n}{Z(D_n)}$$

$$\Rightarrow O(I_{nn} D_n) = \frac{O(D_n)}{O(Z(D_n))} = \frac{2n}{1} = 2n$$

Case-II: If n is even then

$$I_{nn}(D_n) \approx \frac{D_n}{Z(D_n)}$$

$$\Rightarrow O(I_{nn}(D_n)) \approx \frac{O(D_n)}{O(Z(D_n))} = \frac{\cancel{2}n}{\cancel{2}} = n$$

Q. No. of Inner Automorphism in D_4?

Solution: $O(I_{nn} D_4) = \dfrac{O(D_4)}{O(Z(D_4))} = \dfrac{8}{2} = 4$

Q. How many Inner Automorphism in $S_{n,n\geq 3}$?

Solution:

$$I_{nn}(S) \approx \frac{S_n}{Z(S_n)}$$

$$O(I_{nn}(S_n)) = \frac{O(S_n)}{O(Z(S_n))} = \frac{n!}{1} = n!$$

$$I_{nn}(S_n) \approx S_n$$

Q. How many inner automorphism in $U(n)$?

Solution:

Exactly one inner automorphsim because $U(n)$ is abelian.

Q. $f : Z_{16} \times Z_2 \rightarrow Z_8 \times Z_4$ how many onto homomorphism?

Solution:

$f : Z_{16} \times Z_2 \rightarrow Z_8 \times Z_4$ is onto homomorphism

$$\frac{G}{\ker f} \approx G'$$

Here $O(G) = 32, O(G') = 32$

$$\frac{Z_{16} \times Z_2}{\ker f} \approx Z_8 \times Z_4$$

$$O\left(\frac{Z_{16} \times Z_2}{\ker 5}\right) = O(Z_8 \times Z_4)$$

$$\Rightarrow \frac{\cancel{32}}{O(\ker f)} = \cancel{32} \Rightarrow 0(\ker f) = 1$$

$$\Rightarrow \ker f = \{(0,0)\}$$

$$\frac{Z_{16} \times Z_2}{\{(0,0)\}} = \{(a,b) \cdot \{(0,0)\} | (a,b) \in Z_{16} \times Z_2\}$$

$$\approx Z_{16} \times Z_2$$

$$\Rightarrow Z_{16} \times Z_2 \approx Z_8 \times Z_4$$

But $Z_{16} \times Z_2$ has elements or order 16 and $Z_8 \times Z_4$ has no elements of order 16

$$\Rightarrow Z_{16} \times Z_2 \not\approx Z_8 \times Z_2$$

So, onto homomorphism does not exist.

[2] The G/Z theorem:

Let G be a group and $Z(G)$ be the centre of G. If $G/Z(G)$ is cyclic group, then G is Abelian group.

Exam Point: In group theory; proofs become easy to learn; if you are clear about definitions.
Just underline keywords in the statement recall definition and visualize it.

Proof: Let $gZ(G)$ be a generator of $G/Z(G)$ and let $a, b \in G$.
Then there exist integers *i* and *j* such that

$$aZ(G)\left(g^{Z(G)}\right)^i = g^{iz(G)}$$

$$bZ(G) = \left(g^{Z(G)}\right)^j = g^j Z(G)$$

Thus,

$a = g^i x$ for some *x* in $Z(G)$ and $b = g^j y$ for some *y* in $Z(G)$.

$$\therefore \quad ab = \left(g^i x\right)\left(g^j y\right)$$

Now visualize definition of $Z(G)$

$$ab = g^i\left(g^j x\right)y$$

$$= \left(g^i g^j\right)(xy)$$

$$= \left(g^j g^i\right)(yx)$$

$$= \left(g^j y\right)\left(g^i x\right)$$

$ab = ba \Rightarrow G$ is abelian.

<u>**Exam Point**</u>:

(1) If G|H is cyclic where H is a subgroup of $Z(G)$, then G is Abelian.

(2) It is the contra positive of above theorem which is often used - If G is non-abelian then G|Z(G) cannot be cyclic.

[3] For any group G, $G/Z(G)$ is isomorphic to Inn (G).

Hint:

- Consider the correspondence from $G/Z(G)$ $\rightarrow$ Inn(G) given by $T : gZ(G) \rightarrow \phi_g$, where $\phi_g(x) = gxg^{-1}$ for all *x* in G.
- Now just show T is well defined function, one-one onto and operation preserving.

Q. Show that $G_1 \times G_2 \approx G_2 \times G_1$

Solution:

$f : G_1 \times G_2 \rightarrow G_2 \times G_1$ defined by $f(x, y) = (y, x)$

(i) *f* is homomorphism : $(x_1, y_1) \in G_1 \times G_2$

$\left(x_2, y_2\right) \in G_1 \times G_2$

$f\left(\left(x_1, y_1\right)\left(x_2, y_2\right)\right)= f\left(\left(x_1 x_2, y_1 y_2\right)\right)$

$=\left(y_1 \cdot y_2, x_1 \cdot x_2\right)$

$=\left(y_1, x_2\right) \cdot\left(y_2, x_2\right)$

$= f\left(x_1, y_1\right) \cdot f\left(x_2, y_2\right)$

$\Rightarrow f\left(x_1, y_1\right) \cdot\left(x_2, y_2\right)= f\left(x_1, y_1\right) \cdot f\left(x_2, y_2\right) \ \forall x_1, x_2 \in G_1,\ y_1, y_2 \in G_2$

f is homomorphism.

(ii) f is one-one:

$f\left(x_1, y_1\right)= f\left(x_2, y_2\right)$

$\Rightarrow\left(y_1, x_1\right)=\left(y_2, x_2\right)$[$\because$ *f* is homomorphism]

$\Rightarrow y_1=y_2$

$x_1=x_2$

$\Rightarrow\left(x_1, y_1\right)=\left(x_2, y_2\right)$

$\therefore f$ is one-one.

(iii) *f* is onto:

Let $(y, x) \in G_2 \times G_1$ then

$\exists(x, y) \in G_1 \times G_2$ s.t $f(x, y)=(y, x)$

then *f* is onto.

f is homomorphism, one-one and onto then *f* is isomorphism.

Then, $G_1 \times G_2 \approx G_2 \times G_1$

Note: Direct Product of two cyclic group need not be cyclic.

$G_1=Z_8$ is cyclic group of order 8

$G_2=Z_4$ is cyclic group of order 4

$G_1 \times G_2=Z_8 \times Z_4$ is not cyclic because $O\left(Z_8 \times Z_4\right)=32$ but $Z_8 \times Z_4$ has not element of order 32.

Q. Direct Product of two abelian groups is abelian.

Solution:

Let G_1 and G_2 be two abelian groups

$G_1 \times G_2=\left\{\left(g_1, g_2\right) \mid g_i \in G_1, g_2 \in G_2\right\}$

Let $\left(x_1, y_1\right) \in G_1 \times G_2$ and $\left(x_2, y_2\right) \in G_1 \times G_2$

$\left(x_1, y_1\right)\left(x_2, y_2\right)=\left(x_1 x_2, y_1 y_2\right)$

$=\left(x_2 \cdot x_1, y_2 \cdot y_1\right)$[$\because G_1$ and G_2 is abelian]

$=\left(x_2, y_2\right)\left(x_1, y_1\right)$

$\left(x_1, y_1\right)\left(x_2, y_2\right)=\left(x_2, y_2\right)\left(x_1, y_1\right)$

Then $G_1 \times G_2$ is abelian.

Q. Converse if $G_1 \times G_2$ is abelian then G_1 and G_2 is abelian.

Solution:

Since $G_1 \times G_2$ is abelian then let

$G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_1\}$

as $G_1 \times G_2$ is abelian so,

$(x_1, y_1)(x_2, y_2) = (x_2, y_2)(x_1, y_1)$

$\Rightarrow (x_1x_2, y_1y_2) = (x_2x_1, y_2y_1)$

$\Rightarrow x_1x_2 = x_2x_1, \quad x_1, x_2 \in G_1$

and $y_1y_2 = y_2y_1, y_1, y_2 \in G_2$

$\Rightarrow x_1x_2 = x_2x_1, \quad \forall x_1, x_2 \in G_1 \Rightarrow G_1$ is abelian and $y_1y_2 = y_2y_1, \forall y_1, y_2 \in G_2$ then G_2 is abelian.

Note: If G_1 and G_2 be two finite cyclic groups of order *m* and *n*, respectively and $\gcd(m,n) = 1$, then $G_1 \times G_2$ is cyclic.

Solution:

G_1 is finite cyclic group of order *m*

$\Rightarrow G_1 \approx Z_m$

and G_2 is finite cyclic group of order *n*

$\Rightarrow G_2 \approx Z_n$

$G_1 \times G_2 \approx Z_m \times Z_n$ ....(1)

if $\gcd(m,n) = 1$ then $Z_m \times Z_n$ has elements of order mn

$\Rightarrow Z_m \times Z_n \approx Z_{mn}$

$\Rightarrow G_1 \times G_2 \approx Z_{mn}$

$\therefore G_1 \times G_2$ is cyclic

Q. Show that $Z \approx 2Z$.

Solution:

$f : Z \to 2Z$

$f(x) = 2x$

f is homomorphism, one-one and onto.

Then *f* is isomorphism.

then $Z \approx 2Z$

Similarly,

$Z \approx mZ$, where $m = 1, 2, 3....$

Q. Is $(Z,+) \approx (Q,+)$?

Ans. No, because Z is cyclic and Q is not cyclic

i.e. $(Z,+)$ is cyclic group but $(Q,+)$ is not cyclic

$(Z,+) \not\approx (Q,+)$

Note: Similarly, $(Z,+) \not\approx (\mathbf{R},+), (Z,+) \not\approx (\mathbf{C},+)$

$(Z,+) \not\approx R \times Q$ etc.

Q. Is $Z \approx 6Z$?

Solution: Yes, $6Z$ is infinite cyclic group then

$6Z \approx Z$

Q. Is $4Z \approx 6Z$?

Solution: Yes, $4Z \approx Z$

and $6Z \approx Z$

$\Rightarrow 4Z \approx Z \approx 6Z$

$\Rightarrow 4Z \approx 6Z$ (Using Transitive Relation)

Note: Isomorphism is an equivalence relation.

Note: $mZ \approx nZ$, $m \neq 0, n \neq 0$

Q. Is $(Q,+) \approx (Q^* \cdot)$?

Solution:

No, $(Q+) \not\approx (Q^* \cdot)$ because $(Q,+)$ has exactly 1 element of finite order. But $(Q^*,\cdot)$ has 2 elements of order finite.

Q. Is $(Q,+) \approx (R,+)$?

Solution:

No, $(Q,+) \not\approx (R,+)$ because Q is countable but R is uncountable.

Q. Is $(Q,+) \approx (R^*,\cdot)$?

Solution:

No

Q. Is $(Q^*,\cdot) \approx (R^*,\cdot)$? Similarly $(R+) \approx (R^* \cdot)$

Ans. No

Q. (i) $(\mathbf{R},+) \approx (C^*,\cdot)$

(ii) $(\mathbf{C},+) \approx (C^*,\cdot)$

Solution:

(ii) $(\mathbf{C},+) \not\approx (C^*,\cdot)$ because $(\mathbf{C},+)$ has exactly one element of finite order. But $(\mathbf{C}^*,\cdot)$ has infinite number of elements of finite order.

(i) Similarly, $(\mathbf{R},+) \not\approx (C^*,\cdot)$.

Q. $(\mathbf{R},+) \approx (\mathbf{C},+)$?

(1) $\frac{G_1}{\{e\}} \approx G_1$ (2) $\frac{G_1}{G_1} \approx \{e\}$

(3) $\frac{G_1 \times G_2}{\{e_1\} \times G_2} \approx G_1$ (4) $\frac{G_1 \times G_2}{G \times \{e_2\}} \approx G_2$

Q. Show that $G_1 \times \{e_2\}$ is normal subgroup of $G_1 \times G_2$.

Solution:

$G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$ and $G_1 \times \{e_2\} = \{(g_1, e_2) | g_1 \in G_1, e_2 \in G_2\}$

Let $(x, y) \in G_1 \times G_2$ and $(h, e_2) \in G_1 \times \{e_2\}$

$(x, y)(h, e_2)(x, y)^{-1} = (x, y)(h, e_2)(x^{-1}, y^{-1})$

$= (xhx^{-1}, ye_2y^{-1})$

$= \left(xhx^{-1}, e_2\right) \in G_1 \times \{e_2\}$

$\begin{pmatrix} x \in G_1, h \in G_1 \\ \Rightarrow xhx^{-1} \in G_1 \end{pmatrix}$

Then, $G_1 \times \{e_2\}$ is Normal subgroup of $G_1 \times G_2$.

<u>For Finite Group</u>:

Step 1: $O(G_1) = O(G_2)$ if yes

Step 2: G_1 and G_2 both abelian/cyclic. If yes then

Step 3: Find number of elements of possible order in G_1 and G_2

If number of elements of all possible orders in G_1 and G_2 are same then $G_1 \approx G_2$ otherwise not.

Q. $G_1 = Z_8$, $G_2 = Z_2 \times Z_4$, then $G_1 \approx G_2$?

Solution:

$O(G_1) = O(G_2) = 8$

then $G_1 = Z_8$ is cyclic but $G_2 = Z_2 \times Z_4$ is not cyclic then

$Z_8 \not\approx Z_2 \times Z_4$

Q. Is $U(8) \approx U(10)$?

Solution:

$O(U(8)) = 4$

$O(U(10)) = 4$

then $U(8) \approx Z_2 \times Z_2$

$U(10) \approx Z_4$

$U(10)$ is cyclic but $U(8)$ is not cyclic then

$U(8) \not\approx U(10)$.

Q. $G = S_3 \times \frac{Z}{2Z} \approx ?$

(a) Z_{12} (b) $Z_2 \times Z_6$ (c) D_6 (d) $D_3 \times Z_2$

Solution:

$G = S_3 \times \frac{Z}{2Z} \approx S_3 \times Z_2$

$\Rightarrow S_3 \times Z_2$ is non-abelian

$O(S_3 \times Z_2) = 6 \times 2 = 12$

(a) $S_3 \times Z_2 \not\approx Z_{12}$, because Z_{12} is cyclic but $S_3 \times Z_2$ is not cyclic

(b) $S_3 \times Z_2 \not\approx Z_2 \times Z_6$ because $Z_2 \times Z_6$ is abelian but $S_3 \times Z_2$ is non-abelian.

(c) Is $S_3 \times Z_2 \approx D_6$

$O(S_3 \times Z_2) = 12 = O(D_6)$

then $S_3 \times Z_2$ and D_6 both are non-abelian possible order of elements in $S_3 \times Z_2$ are 1,2,3 and 6

Possible order of elements in D_6 are 1,2,3 and 6

No. of elements of order 1 in $S_3 \times Z_2 = 1$

No. of elements of order 2 in $S_3 \times Z_2 = 7$

$1\ 2 = 1 \cdot \phi(2) = 1$

$2\ 1 = 3 \cdot \phi(1) = 3$

# of elements of order 3 in $S_3 \times Z_2 = 2$

$3\ 1 = 2 \cdot \phi(1) = 2$

# of elements of order 6 in $S_3 \times Z_2 = 2$

$3\ 2 = 2 \cdot \phi(2) = 2$

# of elements of order 1 in $D_6 = 1$

order 2 in $D_6 = n + 1 = 7$

order 3 in $D_6 = \phi(3) = 2$

order 6 in $D_6 = \phi(6) = 2$

then $S_3 \times Z_2 \approx D_6$

Similarly, $S_3 \times Z_2 \approx D_3 \times Z_2$

i.e. $S_3 \times Z_2 \approx D_6$ and $S_3 \times Z_2 \approx D_3 \times Z_2$

Q. $S_3 \times \dfrac{Z}{2Z} \approx ?$

(a) Z_{12} (b) $Z_2 \times Z_6$ (c) A_4 (d) D_6

Solution:

$S_3 \times \dfrac{Z}{2Z} \not\approx Z_{12}$ and $Z_2 \times Z_6$ because

$S_3 \times \dfrac{Z}{2Z}$ is non-abelian but Z_{12} and $Z_2 \times Z_6$ is abelian.

Now, checking $S_3 \times \dfrac{Z}{2Z} \approx A_4$

Step 1: $0\left(S_3 \times \dfrac{Z}{2Z}\right) = 0(A_4) = 12$, yes

Step 2: $S_3 \times \dfrac{Z}{2Z}$ and A_4 both are non-abelian

Step3: # of elements of order 2 in $S_3 \times \dfrac{Z}{2Z} = 7$

but # of elements of order 2 in $A_4 = 3$ then $S_3 \times \dfrac{Z}{2Z} \not\approx A_4$

Q. $Z_3 \times D_{11} \approx D_{33}$?

Solution: $O(Z_3 \times D_{11}) = O(D_{33}) = 66$ yes

then

# of elements of order 2 in $Z_3 \times D_{11}$

$1\ 2\ \phi(1) \cdot 11 = 11$

#of elements of order 2 in $D_{33} = 33$

$11 \neq 33$

then

$Z_3 \times D_{11} \not\approx D_{33}$

Q. $Z_{11} \times D_3 \approx D_{33}$?

Solution:

# of elements of order 2 in $Z_{11} \times D_3 = 3$

# of elements of order 2 in $D_{33} = 33$

$3 \neq 33$

then $Z_{11} \times D_3 \not\approx D_{33}$

Q. (i) $Z_3 \times Z_9 \approx Z_{27}$?

(ii) $Z_3 \times Z_5 \approx Z_{15}$?

Solution:

(i) $Z_3 \times Z_9 \not\approx Z_{27}$ because $Z_3 \times Z_9$ is not cyclic and Z_{27} is cyclic.

(ii) $Z_3 \times Z_5 \approx Z_{15}$, because $Z_3 \times Z_5$ and Z_{15} both are cyclic as $\gcd(3,5) = 1$

So $Z_3 \times Z_5 \approx Z_{3\times5} \approx Z_{15}$

Q. $U(8) \approx U(12)$?

Solution:

$U(8) \approx Z_2 \times Z_2$

$U(12) \approx Z_2 \times Z_2$

$\Rightarrow U(8) \approx Z_2 \times Z_2 \approx U(12)$

$\therefore U(8) \approx U(12)$

Q. (i) $S_4 \approx D_{12}$ (ii) $S_3 \times S_4 \approx S_6$

Solution:

(i) $S_4 \not\approx D_{12}$, because S_4 has 9 elements of order 2 and D_{12} has 13 elements of order 2.

(ii) $O(S_3 \times S_4) = O(S_3) \times O(S_4) = 6 \times 24 = 144$

and $O(S_6) = 6! = 720$

$\therefore S_3 \times S_4 \not\approx S_6$.

Q. $G = U(15) \times Z_{10} \times S_5$. Find $O(2,3,(123)(15))$ in G and also find inverse of $(2,3,(123)(15))$.

Solution:

$(2,3,(123)(15)) \in U(15) \times Z_{10} \times S_5$

$\Rightarrow (2,3,(1523)) \in U(15) \times Z_{10} \times S_5$

$\Rightarrow O(2,3,(1523)) = LCM(O(2), O(3), O(1523))$

$= LCM(4,10,4)$

$= 20$

$(2,3,(1523))^{-1} = (8,7,(3251))$

Q. $G_1 = Z_{10} \approx ?$

(i) D_5 (ii) $Z_2 \times Z_4$ (iii) $Z_2 \times Z_5$ (iv) None

Solution:

$O(G_1) = 10,\ O(G_2) = O(Z_2 \times Z_5) = 10$

FUNDAMENTAL THEOREM OF HOMOMORPHISM

If $f : G \to G'$ is onto homomorphism then

$$\frac{G}{\ker f} \approx G'$$

If $f : G \to G'$ is homomorphism then

$$\frac{G}{\ker f} \approx \operatorname{Im} f$$

Q. $f : G \to G'$ is homomorphism and $O(G) = 20$ and $O(G') = 25$. Find possible order of $\ker f$?

(1) 2 (2) 2 (3) 3 (4) 4

Solution:

Case - I:

Let $O(\ker f) = 1$ then

$$O\left(\frac{G}{\ker f}\right) = \frac{O(G)}{O(\ker f)} = \frac{20}{1} = 20$$

$\Rightarrow O(\operatorname{Im} f) = 20$

but $O(\operatorname{Im} f) \times O(G')$ i.e. 20×25 then $O(\ker f) \neq 1$

Case II:

If $O(\ker f) = 2$, then

$$O\left(\frac{G}{\ker f}\right) = \frac{O(G)}{O(\ker f)} = \frac{20}{2} = 10$$

but 10×25 then $O(\ker f) \neq 2$.

Case - III

If $O(\ker f) = 3$ then

$$O\left(\frac{G}{\ker f}\right) = \frac{O(G)}{O(\ker f)} = \frac{20}{3} \text{ but } 3 \times 20$$

then $O(\ker f) \neq 3$

Case - IV

If $O(\ker f) = 4$, then

$$O\left(\frac{G}{\ker f}\right)=\frac{O(G)}{O(\ker f)}=\frac{20}{4}=5$$

5|25, so here $O(\ker f)=4$ is possible

Rule: If $O(\ker f)$ divides $O(G)$ then we get the value of $O(\operatorname{Im} f)$ and if $O(\operatorname{Im} f)$ divides $O(G')$ then that is the possible order of $O(\ker f)$.

Q. $f: Z \to Z_4$, find no of homomorphism?

Solution:

Since Z is cyclic group then it is abelian so all its subgroup are normal.

Case I: $\ker f=\{0\}$ is subgroup of Z

$$\frac{G}{\ker f}\approx \operatorname{Im} f$$

$$\frac{Z}{\{0\}}\approx Z=\operatorname{Im} f$$

$\operatorname{Im} f$ is not subgroup of Z_4 then $\ker f=\{0\}$ is not possible then no homomorphism exist.

Case II:

If $\ker f=Z$ then

$\frac{G}{\ker f}=\frac{Z}{Z}\approx Z_1$, Z_4 has subgroup or order 1 which is isomorphic to Z_1.

Then

# of elements of order 1 in $Z_4=\phi(1)=1$

Case III

$\ker f=2Z$

$\frac{Z}{2Z}\approx Z_2$, Z_4 has subgroup of order 2 which is isomorphic to Z_2.

Then,

Number of elements of order 2 in $Z_4=\phi(2)=1$

Case - IV

$\ker f=3Z$

$\frac{Z}{3Z}\approx Z_3$, Z_4 has subgroup of order 3?

Ans. No, it does not have subgroup of order 3

Then no homomorphism possible corresponding to the $\ker f=3Z$

Case - V

$\ker f=4Z$

$$\frac{Z}{4Z}\approx Z_4$$

Z_4 has subgroup of order 4? Which is isomorphic to Z_4?

Ans. Yes

# of element of order 4 in $Z_4=\phi(4)=2$

So, Total No. of homomorphisms $=1+1+2=4$

NOTE: $f: Z \to Z_n$ has exactly n homomorphisms.

Q. $f: Z_4 \to Z$, how many homomorphism?

Solution:

Z_4 is cyclic then all subgroup of Z_4 are normal.

Subgroup of Z_4 are $H_1 = \{0\}, H_2 = \{(0,2)\}$ $H_3 = Z_4$

Case I: $\ker f = H_1 = \{0\}$

$\frac{Z_4}{\{0\}} \approx Z_4$

but Z has no subgroup of order 4 then

$\ker f \neq \{0\}$ i.e. $\ker f = \{0\}$ is not possible.

Case - II

$\ker f = H_2 = \{(0,2)\}$

$\frac{Z_4}{\{(0,2)\}} \approx Z_2$

but Z has no subgroup of order 2 then $\ker f \neq \{(0,2)\}$ i.e. $\ker f = \{(0,2)\}$ is not possible.

Case - III

$\ker f = H_3 = Z_4$

$\frac{Z_4}{Z_4} \approx Z_1$

here Z has subgroup of order 1 which is isomorphic to Z_1.

Then, Number of elements or order 1 in $Z = 1$

Total No. of Homomorphism = 1

NOTE: Number of Homomorphism from $f: Z_n \to Z$ is exactly 1.

Q. How many homomorphism from $f: S_3 \to Z_6$

Solution:

Normal subgroup of S_3 are:

$H_1 = \{I\}, H_2 = A_3, H_3 = S_3$

Case I:

$\ker f = \{I\}$

$\frac{S_3}{\{I\}} \approx S_3$ and Z_6 has subgroup of order 6 which is not isomorphic to S_3.

So $\ker f = \{I\}$ is not possible.

Not, isomorphic because subgroup of cyclic group is cyclic but S_3 is non-abelian

$\Rightarrow \ker f = \{I\}$ is not possible then no homomorphism exist.

Case- II:

$\ker f = A_3$

$\frac{S_3}{A_3} \approx Z_2$

Q. Z_6 has subgroup of order 2, which is isomorphic to Z_2?

Ans. Yes

Number of elements of order 2 in $Z_6 = \phi(2) = 1$

Case III

$\ker f = S_3$

$\frac{S_3}{S_3} \approx Z_1$

Q. Z_6 has subgroup of order 1, which is isomorphic to Z_1?

Ans. Yes

Number of elements of order 1 in $Z_6 = \phi(1) = 1$

Total No. of homomorphisms $= 1 + 1 = 2$

NOTE: $f : S_3 \to Z_n$

No. of homomorphism = 1, *n* is odd

= 2, *n* is even.

(*n* in Z_n we will check)

Q. $f : Z_6 \to S_3$, how many homomorphism?

Solution:

Normal subgroup of Z_6 are since Z_6 is cyclic.

$H_1 = \{0\}$, $H_2 = \{(0,2,4)\}$, $H_3 = \{(0,3)\}$, $H_4 = Z_6$

Case I:

$\ker = \{0\}$

$\frac{Z_6}{\{0\}} \approx Z_6 = \operatorname{Im} f$

Q. S_3 has subgroup of order 6, which is isomorphic to Z_6?

Ans. It has no subroup or order 6 which is isomorphic to Z_6 i.e. $\not\approx Z_6$.

then $\ker f = \{0\}$, not possible.

Case - II

$\ker f = \{0,2,4\} = \langle 2 \rangle$

$\frac{Z_6}{\{0,2,4\}} = \frac{Z_6}{\langle 2 \rangle} \approx Z_2$

S_3 has subgroup of order 2 which is isomorphic to Z_2

then Number elements of order 2 in $S_3 = 3$.

Case - III

$\ker f = \{0,3\} = \langle 3 \rangle$

$\frac{Z_6}{\langle 3 \rangle} \approx Z_3$

and S_3 has subgroup of order 3 which is isomorphic to Z_3.

Number of elements of order 3 in $S_3 = 2$

Case - IV

$\ker f = Z_6$

$\frac{Z_6}{Z_6} \approx Z_1$

S_3 has subgroup of order 1 then

#of elements of order 1 in $S_3 = 1$

Total No. of homomorphism $= 3 + 2 + 1 = 6$

Q. $f : \frac{Z}{9Z} \times \frac{Z}{4Z} \to \frac{Z}{5Z} \times \frac{Z}{6Z}$, find no. of homomorphism?

Solution: $f : Z_9 \times Z_4 \to Z_5 \times Z_6$

$f : Z_{36} \to Z_{30}$

$= \gcd(36, 30) = 6$

Q. $f : U(11) \times \frac{Z}{3Z} \to U(11) \times \frac{Z}{9Z}$

how many homomorphism?

Solution:

$f : Z_{10} \times Z_3 \to Z_{10} \times Z_9$

$f : Z_{30} \to Z_{90}$

$\gcd(30, 90) = 30$

Q. How many homomorphism in $f : GL_2(\mathbf{F}_2) \to U(7)$?

Solution:

$f : GL_2(\mathbf{F}_2) \to U(7)$

$f : S_3 \to Z_6$

No. of homomorphism = 2, as n is even in Z_6.

Q. $f : U(11) \to U(13)$, how many onto homomorphism?

Solution:

$f : U(11) \to U(13)$

i.e. $f : Z_{10} \to Z_{12}$

Since 12 does not divide 10 hence no onto homomorphism exist.

Q. $f: U(13) \to U(7)$, how many onto homomorphism?
Solution:
$f: Z_{12} \to Z_6$, i.e. $U(13) \approx Z_{12}, U(7) \approx Z_6$
6|12, then # of onto homomorphism $= \phi(6) = 2$
Q. Homomorphic image of abelian group is abelian i.e.
$f: G \to G'$ is an onto homomorphism, if G is abelian then G' is abelian.
Solution:
Let $f: G \to G'$ is onto homomorphism and G is abelian then $xy = yx,\ \forall x, y \in G$
Let $f(x) \in G'$
$f(y) \in G'$
$f(x) \cdot f(y) = f(xy)$ [$\because f$ is homomorphism]
$= f(yx)$ $[xy = yx, \because \text{G is abelian}]$
$= f(y) \cdot f(x)$
$\Rightarrow f(x) \cdot f(y) = f(y) \cdot f(x),\ \forall f(x), f(y) \in G'$ then G' is abelian. [Proved]

<u>Converse of the above theorem need not be true</u>
$f: S_3 \to Z_2$ with $\ker f = A_3$ then
$\frac{S_3}{A_3} \approx Z_2$
i.e. $f(S_3) \approx Z_2$ with $\ker f = A_3$
Z_2 is abelian but S_3 is non-abelian.
Q. Homomorphic image of cyclic group is cyclic but converse need not be true.
i.e. $f: G \to G'$ is onto homomorphism and G is cyclic then G' is cyclic.
Solution:
Let $f: G \to G'$ is homomorphism and G is cyclic then $\exists a \in G$ s.t. $G = \langle a \rangle$
$f(x) \in G',\ x \in G \Rightarrow x = a^n,\ n \in Z$
$\Rightarrow f(x) = f(a^n)$
$= f(a_1, a_2 .... a_n)$ n times
$= f(a) \cdot f(a) ...... f(a)$ [f is homomorphism]
$= (f(a))^n$, where $n \in Z$
then $G' = \langle f(a) \rangle$
then G' is cyclic.
NOTE: Converse of above statement need not be true.
Example: $f: S_4 \to Z_1$ with $\ker f = S_4$
$\frac{S_4}{S_4} = \{IS_4\} \approx Z_1$ (RHS)
Z_1 is cyclic but S_4 is not cyclic.

Q. $f : S_4 \to Z_2$ is onto homomorphism? If yes then find $\ker f$?
Solution:
$f : S_4 \to Z_2$ onto homomorphism exist with $\ker f = A_4$
$\frac{S_4}{A_4} = \{IA_4, \text{odd permutation } A_4\} \approx Z_2 \approx Z_2$ (RHS)
Q. $f : A_4 \to Z_2$, is onto homomorphism? If yes then find $\ker f$?
Solution:
No, onto homomorphism exists because A_4 have no normal subgroup of order 6.
Q. $f : Z_6 \times Z_2 \to S_3$, how many onto homomorphism.
Solution:
We know that homomorphic image of abelian group is abelian.
Since $Z_6 \times Z_2$ is abelian then Image of *f* is abelian and S_3 is non-abelian then onto homomorphism does not exist.
Q. $f : Z_{16} \to Z_2 \times Z_2$, how many onto homomorphism?
Solution:
We know that homomorphic image of cyclic group is cyclic then
Since Z_{16} is cyclic then image of *f* is cyclic but $Z_2 \times Z_2$ is not cyclic then no onto homomorphism exists.
Q. $f : Z_{16} \times Z_2 \to Z_4 \times Z_4$, how many onto homomorphism?
Solution:
No, does not exist $f : G \to G'$
Let $G = Z_{16} \times Z_2$, $G' = Z_4 \times Z_4$, $O(G') = 16, O(G) = 32$
$\frac{G}{\ker f} \approx G'$ $O(\ker f) = 2$
We have no $\ker f$ s.t. $\frac{Z_{16} \times Z_2}{\ker f}$
which is not to $\approx Z_4 \times Z_4$
$\therefore$ No onto homomorphism exist.
Q. Let G be an abelian group of order *n*.
A mapping $f : G \to G$ defined by $f(x) = x^m$ is isomorphism if $\gcd(m, n) = 1$
Solution:
Let $O(G) = n$ and G is abelian then
$\Rightarrow xy = yx, \forall x, y \in G$
$f : G \to G$ defined by
$f(x) = x^m$
(i) f is homomorphism:
$f(xy) = (xy)^m$
$= x^m y^m$ (G is abelian)
$= f(x) \cdot f(y)$

$f(x \cdot y) = f(x) \cdot f(y), \quad \forall x, y \in G$ then *f* is homomorphism.

(2) *f* is one-one:

Let $f(x) = f(y)$

$\Rightarrow x^m = y^m$

$\Rightarrow x^m y^{-m} = e$

$\Rightarrow (xy^{-1})^m = e$

$\Rightarrow O(xy^{-1}) | m$ ....(1)

$[a \in G, a^m = e \because O(a) | m]$

Let $x \in G, y \in G \Rightarrow y^{-1} \in G$ [Since G is group]

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

$\Rightarrow O(xy^{-1}) | O(G)$

$\Rightarrow O(xy^{-1}) | n$ ....(2)

From equation (1) and (2)

$O(xy^{-1}) | m$ and $O(xy^{-1}) | n$

then $\Rightarrow O(xy^{-1}) | \gcd(m,n)$

i.e. $O(xy^{-1}) | \gcd(m,n)$

$\Rightarrow O(xy^{-1}) | 1$, where $\gcd(m,n) = 1$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$

then *f* is one-one.

(3) *f* is onto: $f : G \to G$ and G is finite, if *f* is one-one then *f* is onto.

$\Rightarrow f$ is onto ($\because f$ is one-one)

$\Rightarrow f$ is isomorphism.

Q. $f : Z_{20} \to Z_{20}$ defined by $f(x) = 7x$ is isomorphism?

Solution:

Since $\gcd(7, 20) = 1$ then

$f(x) = 7x$ is isomorphism.

Q. $f : Z_{20} \to Z_{20}$, defined by $f(x) = 5x$ is isomorphism?

Solution:

$f(x) = 5x$ is homomorphism but not one-one ($f(0) = 0$ and $f(4) = 0$ but $0 \neq 4$)

then $f(x) = 5x$ not onto.

Hence, it is not isomorphism.

Conjugate Elements: Let $a,b \in G$, we say that a,i conjugate of b if $\exists$ some $x \in G$ such that $b = xax^{-1}$. If a is conjugate to b $(a \sim b)$ then $\exists x \in G$ s.t. $b = xax^{-1}$ or $x^{-1}ax$.

Q. Show that conjugate Relation $(\sim)$ is an equivalence relation.

Solution:

Reflexive: $e \in G$ s.t. $a = eae^{-1}$ then $a \sim a$.

Symmetric: IF $a \sim b$, then $\exists x \in G$ s.t.

$b = xax^{-1}$

$\Rightarrow xb\left(x^{-1}\right)^{-1} = 0$

$\Rightarrow a = x^{-1}bx,\ x \in G \Rightarrow x^{-1} \in G$

$\Rightarrow b \sim a$

Transitive: If $a \sim b$ and $b \sim c$ then $a \sim c$.

$a \sim b$ then $\exists x \in G$ s.t. $b = xax^{-1}$ ....(1)

and $b \sim c$ then $\exists y \in G$ s.t. $c = yby^{-1}$ ....(2)

From (1) and (2)

$c = yxax^{-1}y^{-1}$

$= (yx)a(yx)^{-1}\ (x \in G, y \in G \Rightarrow xy \in G)$

$c = zaz^{-1}\ (z = yx \in G)$

then $a \sim c$.

<u>Conjugate Class</u>

Definition: Let $a \in G$, then conjugate class of 'a' is denoted by $Cl(a)$ and defined by

$Cl(a) = \{yay^{-1} | y \in G\}$

Note: $e \in G$, then $Cl(e) = \{yey^{-1} | y \in G\}$

$= \{yy^{-1} | y \in G\} = \{e\}$

then $O(Cl(e)) = 1$

Note: (i) If G is abelian and $a \in G$ then

$Cl(a) = \{yay^{-1} | y \in G\}$

$= \{ayy^{-1} | y \in G\}$, since G is abelian $ay = ya$

$= \{ae\}$

$\Rightarrow Cl(a) = \{a\}$

$\Rightarrow O(Cl(a)) = 1$

(ii) If G is cyclic then $Cl(a) = \{e\}$

Note: $a \in G$ then $\bigcup_{a \in G} Cl(a) = G$

$$\Rightarrow 0\left(\sum_{a\in G} Cl(a)\right) = O(G)$$

$$\Rightarrow \boxed{\sum_{a\in G} O\left(Cl(a)\right) = O(G)}$$

Example: $G = Z_{10}, 3 \in Z_{10}$, find $Cl(3)$

$Cl(3) = \{y^3 y^{-1} | y \in G\}$

$= \{3\}$

$O\left(Cl(3)\right) = 1$

i.e. $a \in Z_{10}$, then $Cl(a) = \{a\}$

$O\left(Cl(a)\right) = 1$

$$\sum_{a\in G}\left(Cl(a)\right) = 1+1+1+1+1+1+1+1+1+1$$

$= O(G) = O(Z_{10})$

$$\boxed{\sum_{a\in G} O\left(Cl(a)\right) = O(Z_{10}) = 10}$$

Theorem: If G be a finite group and $a \in G$ then

$$\boxed{O\left(Cl(a)\right) = \frac{O(G)}{O\left(N(a)\right)}}$$

where $N(a) = \{x \in G | xa = ax\}$ or

$C(a) = \{x \in G | xa = ax\}$ i.e. Normalizer of an element $a \in G$.

First class Equation:

$$O\left(Cl(a)\right) = \frac{O(G)}{O\left(N(a)\right)}$$

$$O(G) = \sum_{a\in G} O\left(Cl(a)\right) = \sum_{a\in G} \frac{O(G)}{O\left(N(a)\right)}$$

$$O(G) = \sum_{a\in G} O\left(Cl(a)\right) = \sum_{a\in G} \frac{O(G)}{O\left(N(a)\right)}$$

$$\Rightarrow O(G) = \sum_{a\in G} \frac{O(G)}{O\left(N(a)\right)}$$

$$\Rightarrow O(G) = \sum_{a\in G} i_G\left(N(a)\right)$$

$$i_G\left(N(a)\right) = \frac{O(G)}{O\left(N(a)\right)}$$

Second Class Equation: We know that

$$O(G)=\sum_{a\in G}\frac{O(G)}{O(N(a))}$$

$$\Rightarrow O(G)=\sum_{a\in Z}\frac{O(G)}{O(N(a))}+\sum_{a\notin Z(G)}\frac{O(G)}{O(N(a))}$$

$$\Rightarrow O(G)=O(Z(G))+\sum_{a\notin Z(G)}\frac{O(G)}{O(N(a))}$$

$$O(G)=O(Z(G))+\sum_{a\notin Z(G)}i_G(N(a))$$

Q. $G=Z_4\times Z_2$, write class equation of G.

Solution:

$G=Z_4\times Z_2$ is abelian group

$$\sum_{a\in G}O(Cl(a))=O(G)$$

$$\Rightarrow O(G)=O(Cl(a_1))+O(Cl(a_2))+......+O(Cl(a_8))$$

$$\Rightarrow O(G)=O(Cl(0,0))+0(Cl(0,1))+0(Cl(1,0))+0(Cl(3,0))+0(Cl(3,1))$$

Then,

$$O(G)=\frac{O(G)}{O(N(0,0))}+\frac{O(G)}{O(N(0,1))}+....+\frac{O(G)}{O(N(3,1))}$$

$$=\frac{8}{8}+\frac{8}{8}+\frac{8}{8}+\frac{8}{8}+\frac{8}{8}+\frac{8}{8}+\frac{8}{8}+\frac{8}{8}$$

$$=1+1+1+1+1+1+1+1$$

$$\therefore \boxed{O(Z_4\times Z_2)=1+1+1+1+1+1+1+1}$$

Note: If G is abelian group, then number of conjugate class in $G=O(G)$

Q. $G=D_4$, find conjugate class of each element of D_4.

Solution: $G=D_4=\{R_0,R_{90},R_{180},R_{270},H,V,D,D'\}$

$R_0\in D_4$ s.t.

$$Cl(R_0)=\{yy^{-1}|y\in G\}=\{yy^{-1}|y\in G\}$$

$$=\{R_0\}$$

$$O(Cl(R_0))=1$$

$(R_{90})\in D_4$ s.t.

$$Cl(R_{90})=\{yR_{90}y^{-1}|y\in D_4\}$$

$$=\{R_0R_{90}R_0^{-1},R_{90}R_{90}R_{90}^{-1},R_{180}R_{90}R_{180}^{-1},R_{270}R_{90}R_{270}^{-1},HR_{90}H^{-1},VR_{90}V^{-1},DR_{90}D^{-1}D'R_{90}D'^{-1}\}$$

$$=\{R_{90},R_{90},R_{90},R_{90},R_{270},R_{270},R_{270},R_{270}\}$$

$$Cl(R_{90})=\{R_{90},R_{270}\}$$

$R_{180}\in D_4$

$Cl(R_{180}) = \{yR_{180}y^{-1} | y \in D_4\}$

$Cl(R_{180}) = \{R_{180}\}$

$R_{270} \in D_4$

$Cl(R_{270}) = \{yR_{270}y^{-1} | y \in D_4\}$

$Cl(R_{270} = \{R_{90}, R_{270}\})\ H \in D_4$

$Cl(H) = \{H, V\}$

$Cl(V) = \{H, V\}$

$Cl(D) = \{D, D'\}$

$Cl(D') = \{D, D'\}$

(i) $Cl(R_{90}) = \{R_0\}$

(ii) $Cl(R_{90}) = \{R_{90}, R_{270}\} = Cl(R_{270})$

(iii) $Cl(R_{180}) = \{R_{180}\}$

(iv) $Cl(H) = \{H, V\} = Cl(V)$

(v) $Cl(D) = \{D, D'\} = Cl(D')$

No. of class in $D_4 = 5$

Now, class equation of D_4

$$O(G) = \sum_{a \in G} O(Cl(a)) = O(Cl(R_0)) + O(Cl(R_{90})) + O(Cl(R_{270}))\ O(Cl(H)) + O(Cl(D))$$

$= 1 + 2 + 1 + 2 + 2$

$O(D_4) = 1 + 1 + 2 + 2 + 2$

This is the class equation.

Class Equation of S_3

$S_3 = \{I, (12), (13), (23), (123), (132)\}$

$I \in S_3$

$Cl(I) = \{I\}$

$(12) \in S_3$

$Cl(12) = \{y(12)y^{-1} | y \in S_3\}$

$= \{I(12)I^{-1}, (12)(12)(12)^{-1}, (13)(12)(13)^{-1}(23)(12)(23)^{-1}, (123)(12)(123)^{-1}, (132)(12)(132)\}$

$Cl(12) = \{(12), (12), (23), (13), (23), (13)\}$

$Cl(12) = \{(12), (13), (23)\}$

$Cl(123) = \{y(123)y^{-1} | y \in S_3\}$

$$= \begin{Bmatrix} I(123)I^{-1},(12)(123)(12)^{-1},(13)(123)(13)^{-1} \\ (23)(123)(23)^{-1},(123)(123)(123)^{-1},(132)(123)(132)^{-1} \end{Bmatrix}$$

$Cl(123) = \{(123),(132),(132),(132),(123),(123)\}$

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

No. of conjugate class in $S_3 = 3$

class equation of $S_3 = \sum_{a \in S_3} Cl(a)$

$= O(Cl(I)) + O(Cl(12)) + O(Cl(123))$

$= 1+3+2$

i.e. $O(S_3) = 1+2+3$. This is class equation.

Note: Number of conjugate class in $S_n = P(n)$ i.e. partition of n

No. of conjugate class in $D_n = \begin{cases} \dfrac{n+6}{2}, \text{if } n \text{ is even} \\ \dfrac{n+3}{2}, \text{if } n \text{ is odd} \end{cases}$

Q. Write the class equation of S_4?

Q. If $O(G) = p^n$ then $O(Z(G)) > 1$.

Solution:

Let G be a group and $O(G) = p^n$ ....(1)

Now,

$Z(G) = \{Z \in G \mid xz = zx, \forall x \in G\}$ ....(2)

We know, $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \dfrac{O(G)}{O(N(a))}$ ....(3)

where $N(a) = \{x \in G \mid xa = ax\}$, since $N(a)$ is subgroup of G then by Lagrange's Theorem

$O(N(a)) \mid O(G)$

If $a \notin Z(G)$ then $O(N(a)) = p^k$, $0 < k < n$

$\Rightarrow \dfrac{O(G)}{O(N(a))} = \dfrac{p^n}{p^k} = p^{n-k}$ ....(4)

Now, $\exists p$ such that $p \left| \dfrac{O(G)}{O(N(a))} \right.$

$\Rightarrow p \left| \sum_{a \notin Z(G)} \dfrac{O(G)}{O(N(a))} \right.$ ....(5)

Now,

$p \mid O(G) = p^n$ ....(6)

From equation (5) and (6)

$p \left| O(G) \right.$ and $p \left| \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))} \right.$

$\Rightarrow p \left| O(G) - \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))} \right.$

$\Rightarrow p \left| O(Z(G)) \right.$ [From equation (3)]

$\Rightarrow \boxed{O(Z(G)) > 1}$

Q. If $O(G) = p^3$ and G is non-abelain then $O(Z(G)) =$

(a) 1 (b) p^3 (c) p^2 (d) p

Ans. (b)

$O(Z(G)) = p^3$, then $\frac{O(G)}{O(Z(G))} = \frac{p^3}{p^3} = 1 \approx Z_1$

G is abelain but given G is non-abelian [Also if $O(G) = p^n$ then $O(Z(G)) > 1$]

(a) If $O(G) = p^3$ then $O(Z(G)) \neq 1$ because by theorem $O(Z(G)) > 1$. Hence not possible

(c) If $O(G) = p^3$ and $O(Z(G)) = p^2$ then

$\frac{O(G)}{O(Z(G))} = \frac{p^3}{p^2} = p \approx Z_p$

$\Rightarrow \frac{G}{Z(G)}$ is cyclic G is abelian but G is non-abelian then $O(Z(G)) \neq p^2$.

(d) Therefore, $O(Z(G)) = p$ is correct option.

Example: (i) $O(G) = 8$ and G is non-abelian then $O(Z(G)) = 2$.

(ii) $O(G) = 27$ and G is non-abelian then $O(Z(G)) = 3$

Q. If $O(G) = p^3$, then $O(Z(G)) = ?$

(a) 1 (b) p^3 (c) p^2 (d) p

Solution:

$O(G) = p^3$

Case I: If G is abelian then $O(Z(G)) = O(G) = p^3$

Case II: If G is non-abelain then $O(Z(G)) = p$

Note: $O(Cl(a))$ in $S_n = \frac{O(G)}{O(N(a))} = \frac{\lfloor n}{1^{\alpha_1} \cdot 2^{\alpha_2} \ldots k^{\alpha_k} \lfloor \alpha_1 \lfloor \alpha_2 \ldots 1}$

Class Equation of S_4

Q. $G = S_4$, # of conjugate class in $S_4 = P(4) = 5$

$4 \to (1234)$

$3+1 \to (123)$

$2+2 \to (12)(34)$

$2+1+1 \to (12)$

$1+1+1+1 \to I$

$$O(Cl(1234)) = \frac{O(G)}{O(N(1234))} = \frac{\lfloor 4}{1^{\circ}\cdot 2^{\circ}\cdot 3^{\circ}\cdot 4^{1}\lfloor 1} = \frac{\not{4}\times 3\times 2\times 1}{\not{4}} = 6$$

$$O(Cl(123)) = \frac{\lfloor 4}{1^{\circ}\cdot 2^{\circ}\cdot 3^{1}\cdot \lfloor 1} = \frac{4\times \not{3}\times 2\times 1}{1\times \not{3}} = 8$$

$$O(Cl(12)(34)) = \frac{\lfloor 4}{2^2\lfloor 2} = \frac{\not{4}\times 3\times \not{2}\times 1}{\not{4}\times \not{2}\times 1} = 3$$

$$O(Cl(12)) = \frac{\lfloor 4}{1^2\cdot 2\lfloor 2\lfloor 1} = \frac{\not{4}\times 3\times \not{2}\times 1}{\not{2}\times \not{2}} = 6$$

$$O(Cl(I)) = \frac{\lfloor 4}{1^4\lfloor 4} = 1$$

Class Equation of $S_4 = \sum_{a\in G} O(Cl(a))$

$= O(Cl(I)) + O(Cl(12)) + O(Cl(12)(34)) + O(Cl(123)) + O(Cl(1234))$

$O(S_4) = 1+6+3+8+6$ (Class equation)

$\Rightarrow O(S_4) = 24$

Q. $(12)(34) \in S_n$, $n \geq 4$, find $O(Cl(12)(34))$?

Solution:

$G = S_n$

$n = 2+2+1+1+1+....+1$

$$O(Cl(12)(34)) = \frac{O(G)}{O(N(12)(34))} = \frac{\lfloor n}{1^{n-4}\cdot 2^2\lfloor n-4\lfloor 2}$$

$$= \frac{n(n-1)(n-2)(n-3)\lfloor n-4}{8\lfloor n-4}$$

$$O(Cl(12)(34)) = \frac{n(n-1)(n-2)(n-3)}{8}$$

Q. How many elements commute with $(12)(34)$ in S_n, $n \geq 4$?

Solution:

$$\frac{O(G)}{O(N(a))} = \frac{\lfloor n}{1^{\alpha_1}\cdot 2^{\alpha_2}....k^{\alpha_k}\lfloor \alpha_1\lfloor \alpha_2....\lfloor \alpha_k}$$

$$\frac{\lfloor n}{O(N(a))} = \frac{\lfloor n}{1^{\alpha_1} \cdot 2^{\alpha_2} \ldots . k^{\alpha k} \lfloor \alpha_1 \lfloor \alpha_2 \ldots \lfloor \alpha_k}$$

$$\Rightarrow O(N(a)) = 1^{\alpha_1} \cdot 2^{\alpha_2} \ldots .. k^{\alpha_k} \cdot \lfloor \alpha_1 \cdot \lfloor \alpha_2 \ldots \lfloor \alpha_k$$

$$= 1^{n-4} \cdot 2^2 \lfloor n-4 \lfloor 2$$

$$= 8 \lfloor n-4$$

Q. Let S_{10} denote the group of permutation 10 symbol then the # of elements of S_{10} commute with (13579)

Solution:

$G = S_{10}$

$10 = 5+1+1+1+1+1$

$O(N(13579)) = ?$

$$O(Cl(13579)) = \frac{O(G)}{O(N(13579))} = \frac{\lfloor 10}{1^5 \cdot 5^1 \lfloor 5 \lfloor 1}$$

$$O(Cl(13579)) = \frac{\lfloor 10}{5 \lfloor 5}$$

then $O(N(13579)) = 5\lfloor 5$

Q. $G = U(15)$, find class equation and also find # of conjugate class.

Solution:

$G = U(15)$ is abelian group then

No. of conjugate class = $O(U(15)) = 8$

Note: $O(G) = p^3$ and G is non-abelian then

# of conjugate class in $G = p^2 + p - 1$

Q. $O(G) = 3^3$, find # of conjugate class in G?

(a) 1 (b) 27 (c) 11 (d) 20

Solution:

Case I: $O(G) = 27$ and G is abelian then

# of conjugate class in $G = O(G) = 27$

Case II: $O(G) = 27$ and G is non-abelian then

# of conjugate class $= 3^2 + 3 - 1 = 9 + 3 - 1 = 11$

Q. How many conjugate class in S_5

Solution:

# of conjugate class in $S_5 = P(5)$

5
4+1
3+2
3+1+1
2+2+1

2+1+1+1
1+1+1+1+1
5-conjugate class in S_5.

Q. $f=(123)\in S_n, n\geq 3$, how many elements commute with (123).

Solution:

$n=3+1+1+1+....+1$

# of elements commute with (123) in S_n

$=1^{n-3}\cdot 3^1 \underline{|n-3}\,\underline{|1}$

$=3\underline{|n-3}$

Q. Which of the following is class equation of group
(i) 10 = 1+1+1+2+5
(ii) 4 = 1+1+2
(iii) 8 = 1+1+3+3
(iv) 6 = 1+2+3

Solution:

(b)

if $O(G)=4$ < Z_4, $Z_2\times Z_2$

Class equation is 1+1+1+1 so this is not possible since both are abelian.
If $G\approx Z_4$ then class equation is 1+1+1+1=4
If $G\approx Z_2\times Z_2$ then class equation is 4 = 1+1+1+1
So the class equation given in option is not possible.

(c) $a\in G$ and $O(Cl(a))=3$ then $O(Cl(a))\,|\,O(G)$

$\Rightarrow 3\,|\,8$ but 3×8 then $O(Cl(a))=3$ is not possible if $O(G)=8$

(a)

10 = 1+1+1+2+5

$\Rightarrow O(Z(G))=3$

$\Rightarrow 3\,|\,O(G)\Rightarrow 3\,|\,10$ (By Lagrange Theorem)

[Since $Z(G)$ is subgroup of G then by Lagrange Theorem $O(Z(G))\,|\,O(G)$]

But it is not possible thus 10 = 1+1+1+2+5 is not a class equation.

Note: If $O(Cl(a))=1, a\in G$

$$\Rightarrow \frac{O(G)}{o(N(a))}=1\Rightarrow O(G)=O(N(a))$$

i.e. $a\in Z(G)$

Q. If $O(G)=p^2$, then G is always abelian.

Solution:

Let $O(G)=p^2$ and $Z(G)$ is Centre of group G then by Lagrange, Theorem possible order of $Z(G)$ are 1, p and p^2.

If $O(G) = p^n$, then $O(Z(G)) > 1$ then $O(Z(G)) \neq 1$ then only possible order or $Z(G) = p$ or p^2.

Case I: If $O(Z(G)) = p$, then

$$\frac{O(G)}{O(Z(G))} = p$$

$\Rightarrow \dfrac{G}{Z(G)} \approx Z_p$, as Z_p is abelian

$\Rightarrow G$ is abelian

Case II: If $O(Z(G)) = p^2$ then

$$\frac{O(G)}{O(Z(G))} = 1 \approx Z_1$$

$\Rightarrow G$ is abelian

From case I and II

G is always abelian [Proved].

Existence of elements of prime order.

Statement:
Let G be a finite abelian group and let *p* be a prime that divides the order of G. Then G has an element of order *p*.

Note: Here we'll use the method of mathematical induction on $|G|$

We assume that the statement is true for all abelian groups with fewer elements than G and use this assumption to show that the statement is true for G as well.

Certainly, G has elements of prime order, for if $|x| = m$ and $m = q \cdot n$ where *q* is prime, then $|x|^n = q$. So let *x* be an element of G of some order (prime) *q*, say.
If $q = p$, we are finished; so assume $q \neq p$.
$\because$ every subgroup of an abelian group is normal, we may construct the factor group
$\bar{G} = G/\langle x \rangle$.

Then $\bar{G}$ is abelian and *p* divides $|\bar{G}|$,

$\because |\bar{G}| = |G|/q$.

By induction, $\bar{G}$ has an element call it $y\langle x \rangle$ of order *p*. Thus the coset $y\langle x \rangle$ raised to $p+h$ power is the identity element $\langle x \rangle$ in $\bar{G}$.

i.e. $\left(y\langle x \rangle\right)^p = y^p \langle x \rangle = \langle x \rangle$

It follows, then, that $y^p \in \langle x \rangle$, so that $y^p = e$ or y^p has order *q*. If $y^p = e$, then *y* is the desired element of order *p*; if y^p has order *q* then y^2 has order *p*. In either case, we have produced an element of order *q*.

Exam Point: Such proofs are not easy to remember. But if we decode those by visualizing some standard group then it's easy to understand, then keep revising on different intervals.
Exa. Here think about $U(20)$; abelian group and now think how you take *x*, then what'll be the factor group and then what will be *y*, y^q !

[5] Fundamental Theorem of Finite Abelian Group
Statement: Every finite abelian group is a direct product of cyclic groups of prime power order. Moreover the factorization is unique except for rearrangement of the factors.
Exam Point: Proof is not expected only remember the statement is necessary point.

Use of Fundamental Theorem:
The fundamental theorem is extremely powerful. As an application, we can use it as an algorithm for constructing all abelian groups of any order.
Example: Let's look at groups of order p^k where *p* is a prime and $k \leq 4$.

Order of G	**Partitions of *k***	**Possible Direct Products**
P	1	$\mathbf{Z}_p$
p^2	2 2+1	$\mathbf{Z}p^2$ $\mathbf{Z}p \times \mathbf{Z}p$
p^3	3 2+1	$\mathbf{Z}p^3$

	1+1+1	$\mathbf{Z}p^2 \times \mathbf{Z}p$ $\mathbf{Z}p \times \mathbf{Z}p \times \mathbf{Z}p$
p^4	4 3+1 2+2 2+1+1 1+1+1+1	$\mathbf{Z}p^4$ $\mathbf{Z}p^3 \times \mathbf{Z}p$ $\mathbf{Z}p^2 \times \mathbf{Z}p^2$ $\mathbf{Z}p^2 \times \mathbf{Z}p \times \mathbf{Z}p$ $\mathbf{Z}p \times \mathbf{Z}p \times \mathbf{Z}p \times \mathbf{Z}p$

Example: Let G be an abelian group of order 1176.

$\because 1176 = 2^3 \cdot 3 \cdot 7^2$

Let's write all possible abelian groups (up to isomorphism) of order 1176.

$Z_8 \times Z_3 \times Z_{49}$

$Z_4 \times Z_2 \times Z_3 \times Z_{49}$

$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_{49}$

$Z_8 \times Z_3 \times Z_7 \times Z_7$

$Z_4 \times Z_2 \times Z_3 \times Z_7 \times Z_7$

$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_7 \times Z_7$

[6] Existence of subgroups of Abelian group.

Statement: If *m* divides the order of a finite abelian group, then G has a subgroup of order *m*.
(Remember the statement)

Sylow Theorems Segment

[1] (Sylow's First Theorem) Existence of subgroups of Prime-Power order.

Statement: Let G be a finite group and let *p* be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

[2] (Cauchy's Theorem)

Statement: Let G be a finite group and *p* be a prime that divides the order of G. Then G has an element of order *p*.

[3] (Sylow's Second Theorem)

Statement: If H is a subgroup of a finite group G and $|H|$ is a power of a prime *p*, then H is contained in some Sylow-*p* subgroup of G.

[4] (Sylow's Third Theorem)

Statement: The number of Sylow *p*-subgroups of G is equal to 1 modulo *p* and divides $|G|$. Furthermore, any two Sylow *p*-subgroups of G are conjugate.

[5] (A unique Sylow *p*-subgroup)

Statement: A Sylow *p*-subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow *p* subgroup of G.

[6] (Applications of Sylow Theorems)

Exam Points:

(i) Classification of Groups of order $2p$

Let $|G| = 2p$, where *p* is a prime. Then G is isomorphic to Z_{2p} or D_p

(ii) Cyclic Groups of order p^q

If G is a group of order pq, where p and q are primes, $p < q$ and p does not divide $(q-1)$, then G is cyclic. In particular G is isomorphic to $\mathbf{Z}_{pq}$.

Type: Complete Chapter (24) Sylow Theorems (For Proof

<u>Learning in categories now:</u>

p-group: A group G is said to be p-group if $O(G) = p^n$.

For example:

$O(G) = 64$ is p-group

yes, $O(G) = 2^6 = p^6$, where $p = 2$

<u>Cauchy's Theorem for Finite Abelian Group</u>:

Statement: Let G be a finite abelian group and $p \mid O(G)$ then $\exists e \neq a \in G$ such that $a^p = e$.

Note: If G be a finite abelain group and $p \mid O(G)$ then G has subgroup of order p, which is ismorphic to Z_p.

e.g.

$O(G) = 12$ and G is abelain 2|2, then G has subgroup of order 2.

$$O(G) = 12 \begin{cases} Z_{12} \\ Z_2 \times Z_6 \end{cases}$$

(i) If $G \approx Z_{12}$ then G has unique subgroup of order 2

$\langle 6 \rangle = \{0, 6\} \approx Z_2$

(ii) If $G \approx Z_2 \times Z_6$, then G has subgroup of order 2 because $Z_2 \times Z_6$ has elements of order 2.

# of subgroup of order 2 in $Z_2 \times Z_6 = \dfrac{3}{\phi(2)} = 3$

$H_1 = \langle (0,0) \rangle = \{(0,0), (1,0)\} \approx Z_2$

$H_2 = \langle (0,3) \rangle = \{(0,0), (0,3)\} \approx Z_2$

$H_3 = \langle (1,3) \rangle = \{(0,0), (1,3)\} \approx Z_2$

Again,

$O(G) = 12$, and G is abelian, 3|12, then G has subgroup of order 3

$$O(G) = 12 \begin{cases} Z_{12} \\ Z_2 \times Z_6 \end{cases}$$

(i) If $G \approx Z_{12}$, then G has subgroup of order 3

$H = \langle 4 \rangle$, $\{0,4,8\} \approx Z_3$

(ii) If $G \approx Z_2 \times Z_6$, then G has subgroup of order 3

$H = \langle (0,2) \rangle = \{(0,0),(0,2),(0,4)\} \approx Z_3$

Cauchy's Theorem

If G be a finite group and $p \mid O(G)$ then G has element of order *p*.

Sylow's First Theorem

If G be a finite group and $p^n \mid O(G)$ then G has subgroup of order p^n.

e.g. $O(G) = 56 = 8 \times 7$

$2 \mid O(G)$ then G has subgroup of order 2

$2^2 \mid O(G)$ then G has subgroup of order $2^2 = 4$

$2^3 \mid O(G)$ then G has subgroup of order $2^3 = 8$

$7 \mid O(G)$ then G has subgroup of order 7.

Sylow-p subgroup (p-SSG): Let G be a finite group and $p^n \mid O(G)$ but $p^{n\times 1} \times O(G)$ then G ahs subgroup of order p^n, which is called Sylow's p-subgroup or p-SSG of order p^n.

e.g. $O(G) = 12,\ 2^2 \mid O(G)$ but $2^{2+1} \times O(G)$ then G has 2-SSG of order 4.

Q. $O(G) = 16$, find order of 2-SSG in G?

Solution:

$O(G) = 16 = 2^4$

$2^4 \mid O(G)$ but $2^{4+1} \times O(G)$ then G has 2-SSG of order $2^4 = 16$

Q. $O(G) = 27$, 3-SSG of G is normal?

Solution:

$O(G) = 27$ then $3^3 \mid O(G)$ but $3^{3+1} \times O(G)$ then G has subgroup of order $3^3 = 27$, which is 3-SSG.

$O(3-SSG) = 27 = O(G)$

$\Rightarrow 3-SSG = G$

We know that G, is always normal subgroup of G then 3-SSG is normal subgroup of G.

Q. $O(G) = 8$, 2-SSG of G is normal?

Solution: $O(G) = 8$ then $2^3 \mid O(G)$ but $2^{3+1} \times O(G)$ then G has subgroup of order 2^3, which is 2-SSG

$O(2-SSG) = 8 = O(G)$

$\Rightarrow 2SSG = G$

We know that G is always normal subgroup of G then 2-SSG is normal subgroup of G.

Sylow's Second Theorem

Any two p-SSG of G are conjugate

i.e. If H_1 and H_2 are two p-SSG of G then $\exists x \in G$ (for *x*)

Such that $H_1 = xH_2x^{-1}$ (*p* chosen once only)

Q. $G = S_3 = \{I,(12),(13),(23),(123),(132)\}$

$O(S_3) = 6$ and $2^1 \mid O(G)$ but $2^{1+1} \times O(G)$ then G has 2-SSG of order $2^1 = 2$

2-SSG of S_3, $H_1 = \{I,(12)\}, H_2 = \{I,(13)\}$ $H_3 = \{I,(23)\}$

$H_3 = xH_2x^{-1}$

H_2 is conjugate to H_3

$H_3 = xH_2x^{-1}$

Let $x = (12) \in S_3$

$xH_2x^{-1} = (12)H_2(12)^{-1}$

$= (12)\{I,(13)\}(12)^{-1}$

$= \{(12)I(12)^{-1},(12)(13)(12)^{-1}\}$

$= \{I,(23)\}$

$= H_3$

$(12)(13)(12)^{-1}$

$= \begin{pmatrix} 12 \\ 21 \end{pmatrix}\begin{pmatrix} 13 \\ 31 \end{pmatrix}\begin{pmatrix} 12 \\ 21 \end{pmatrix}$

$= \begin{pmatrix} 12 \\ 21 \end{pmatrix}\begin{pmatrix} 123 \\ 231 \end{pmatrix}$

$= \begin{pmatrix} 123 \\ 132 \end{pmatrix}$

H_1 **is conjugate to** H_2

$H_2 = xHx^{-1}$

Now, $3 \mid O(S_3)$ but $3^{1+1} \times O(S_3)$ then G has 3-SSG of order $3^1 = 3$

\# of 3-SSG in $G = \frac{2}{\phi(3)} = \frac{2}{2} = 1$

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

H is conjugate to H

$H = xHx^{-1}$

$x \in S_3, x = I$ s.t. $xHx^{-1} = IHI^{-1}$

$\Rightarrow H \sim H$

<u>**Sylow's Third Theorem**</u>

Statement: Number of P-SSG (n_p) in G is equal to $1+kp$ such that $1+kp \mid O(G)$ and $k = 0,1,2,....$

i.e. $n_p = 1+k_p$ such that $1+k_p \mid O(G), k = 0,1,2,....$

Q. $O(G) = 6$, find number of 2-SSG in G.

Solution: $O(G) = 6 = 2\times 3, 2^1 \mid O(G)$ but $2^{1+1} \times O(G)$ then G has 2-SSG of order $2^1 = 2$.

No. of 2-SSG in $G(n_2)=1+2k, k=0,1,2,....$

s.t. $1+2k \mid O(G)$

Put $k=0,\ n_2=1+2.0=1$

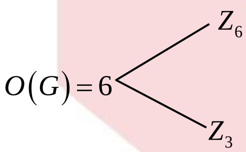
and $1 \mid O(G)$ i.e. 1|6 then $n_2=1$ is possible

put $k=1,\ n_2=1+2=3$ and $3 \mid O(G)$ i.e. 3|6 then $n_2=3$ is possible.

Put $k=2,\ n_2=1+4=5$ and $5\times O(G)$ so $n_2=5$ is not possible.

Similarly, $k=3,4,5,....$ is not possible for 2-SSG.

If $O(G)=6$, then G has either unique 2-SSG or 3, 2-SSG.



If $G\approx Z_6$ then 2-SSG is unique.

If $G\approx S_3$ then 2-SSG is 3.

Q. $O(G)=6$, find # of 3-SSG in G?

Solution:

$O(G)=6=2\times 3,\ 3 \mid O(G)$ but $3^{1+1}\times O(G)$ then G has 3-SSG of order $3^1=3$

No. of 3-SSG in $G(n_3)=1+3k$, $k=0,1,2,....$

s.t. $1+3k \mid O(G)$ i.e. $1+3k \mid 6$

(i) Put $k=0$, $n_3=1+3\cdot 0=1$

1|6, then $n_3=1$ is possible.

(ii) Put $k=1,\ n_3=1+3\cdot 1=4$ but $4\times O(G)$ then $n_3=4$ is not possible for 3-SSG.

Hence, if $O(G)=6$ then G has only unique 3-SSG.

Similarly, for $k=2,3,4,....$ is not possible for 3-SSG.

i.e. if $O(G)=6$, then there is unique 3-SSG in G.

Q. Show that 3-SSG and 5-SSG in G is unique where $O(G)=15$?

Solution:

$O(G)=15=3\times 5$

(i) For 3-SSG

$3' \mid O(G)$ but $3^{1+1}\times O(G)$ then G has 3-SSG of order 3'=3

No. of 3-SSG in $G(n_3)=1+3k$

Put $k=0$, then $n_3=1+3\cdot 0=1$ and $1 \mid O(G)$ then $n_3=1$ is possible for 3-SSG.

Put $k=1$, then $n_3=1+3\cdot 0=1$ and $1 \mid O(G)$ then

$n_3=1$ is possible for 3-SSG.

Put $k=1$, then $n_3=4$ but $4\times O(G)$ then

$n_3 = 4$ is not possible.
Similarly $k = 2,3,4,...$ is not possible for 3-SSG.
Then, G has unique 3-SSG which is $n_3 = 1$.
(ii) For 5-SSG
$5^1 \mid O(G)$ but $5^{1+1} \times O(G)$ then G has 5-SSG of order 5.
Similarly, like 3-SSG, 5-SSG also has unique 5-SSG.
Hence, G has unique 3-SSG and 5-SSG if $O(G) = 15$

Homework
Q1. If $O(G) = 33$ then G has unique 3-SSG and II-SSG
Q2. If $O(G) = 35$ then G has unique 5-SSG and 7-SSG.
Q3. If $O(G) = 77$ then G has unique 7-SSG and II-SSG.
Note: If $O(G) = pq$ and $p \times q^{-1}$ then G has unique P-SSG and q-SSG.
Q. $G = GL_n(\mathbf{F}_4)$, find order of q-SSG in G?
Solution:
$G = GL_n(\mathbf{F}_q)$
$O(G) = 0(GL_n(\mathbf{F}_q)) = (q^n - q^{n-1})(q^n - q^{n-2})....(q^n)$
$= q^{n-1}(q-1)q^{n-2}(q^2-1)...q^0(q^n-1)$
$= q^{(n-1)+(n-2)+....+1+0}(q-1)(q^2-1)....(q^n-1)$
$= q^{0+1+2+....+(n-1)}(q-1)(q^2-1)......(q^n-1)$

$$O(GL_n(\mathbf{F}_4)) = q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)....(q^n-1) \quad ....(1)$$

From (1)
$q^{\frac{n(n-1)}{2}} \Big| O(G)$ but $q^{\frac{n(n-1)}{2}} \times O(G)$
then $G = GL_n(\mathbf{F}_q)$ has q-SSG of order
$q^{\frac{n(n-1)}{2}}$
Q. $G = GL_{50}(\mathbf{F}_q)$, find order of q-SSG
Solution: Order of q-SSG in $G = q^{\frac{50(50-1)}{2}}$
$= q^{49\times 50} = q^{1225}$
Q. $G = SL_n(\mathbf{F}_q)$, find order of q-SSG in G.
Solution:

$$O(SL_n(\mathbf{F}_q)) = \frac{(q^n - q^{n-1})(q^n - q^{n-2}).......(q^n - 1)}{q-1}$$

$$= \frac{q^{\frac{n(n-1)}{2}} \cancel{(q-1)}\left(q^2-1\right).....\left(q^n-1\right)}{\cancel{(q-1)}}$$

$$O\left(SL_n\left(\mathbf{F}_q\right)\right) = q^{\frac{n(n-1)}{2}}\left(q^2-1\right)\left(q^3-1\right).....\left(q^n-1\right)$$

$q^{\frac{n(n-1)}{2}} \Big| O(G)$ but $q^{\frac{n(n-1)}{2}+1} \times O(G)$ then G has q-SSG of order $\boxed{q^{\frac{n(n-1)}{2}}}$

Q. H is unique p-SSG in G iff H is normal subgroup of G.
Solution:
Let H is unique p-SSG in G of order p^n then $p^n \mid O(G)$ but $p^{n+1} \times O(G)$

Let $x \in G$ (*x* is arbitrary) s.t. $k = xHx^{-1}$ is subgroup of G because $O(k) = O\left(xHx^{-1}\right)O(H) = p^n$

Then, by Sylow's 1st theorem, *k* is subgroup of G of order p^n.

Since, $p^n \mid O(G)$ but $p^{n+1} \times O(G)$ then K is also p-SSG of G of order p^n.

But G has unique p-SSG then $k = H$

$\Rightarrow xHx^{-1} = H,\ \forall x \in G$

Then, H is normal subgroup of G.

<u>Conversely</u>, Let H is p-SSG of G and H is normal then $H = xHx^{-1}\ \forall x \in G$ ....(1)

Now, H and K are two p-SSG in G then by Sylow's second theorem $\exists$ some $x \in G$ s.t.

$k = xHx^{-1}$ ....(2)

From (1) and (2)

$k = H$, then H is unique.

Q. $G = \left\{x^i y^j \middle| x^3 = e, y^{13} = e; xy \neq yx, i = 0,1,2, y = 0,1,2,..\right\}$

(i) How many 13-SSG in G?
(ii) 13-SSG in G is normal subgroup of G?
Solution:

(i) $O(G) = 39 = 3 \times 13$ and G is non-abelain $13^1 \mid O(G)$ but $13^{1+1} \times O(G)$ then G has 13-SSG of order $13^1 = 13$.

# of 13-SSG in $G = 1+13k, k = 0,1,....$ and $1+13k \mid O(G)$

Put $k = 0$ then

$n_{13} = 1+13\cdot 1 = 1$ and $1 \mid O(G)$ then $n_{13} = 1$ is possible.

Put $k = 1$, then

$n_{13} = 1+13\cdot 1 = 14$ and $14 \times O(G)$ then $n_{13} = 14$ is not possible.

Similarly, $k = 2,3,4,5,....$ are not possible for 13-SSG.

then G has unique 13-SSG.

(ii) Since 13-SSG in G is unique then 13-SSG of G is normal subgroup of G.

Q. $O(G) = 39$ and G is non-abelian.

(i) How many 3-SSG in G?
(ii) 3-SSG in G is normal.
Solution:

$O(G)=39=3\times 13$ and G is non-abelian group $3^1 \mid O(G)$ but $3^{1+1}\times O(G)$ then G has 3-SSG of order $3^1=3$.

# of 3-SSG in $G=1+3k, k=0,1,2,$ s.t. $1+3k \mid O(G)$

Put $k=0$, then $n_3=1+3\cdot 0=1$ and $1 \mid O(G)$ then $n_3=1$ is possible.

Put $k=1$, then $n_3=1+3\cdot 1=4$ and $4\times O(G)$ then $n_3=4$ is not possible for 3-SSG.

Put $k=2$ then $n_3=1+3\cdot 2=7$ and $7\times O(G)$ then $n_3=7$ is not possible for 3-SSG.

Put $k=3$ then $n_3=1+3\cdot 3=10$ and $10\times O(G)$ then $n_3=10$ is not possible for 3-SSG.

Put $k=4$ then $n_3=1+3\cdot 4=14$ and $13 \mid O(G)$ then $n_3=13$ is possible for 3-SSG.

Similarly, now $k=5,6,....$ are not possible for 3-SSG.

# of 3-SSG in $G=1$ or 13.

Now,

(i) $O(G)=39$ and G is non-abelian then G has 13 subgroups of order 3.

$\Rightarrow G$ has 13, 3-SSG.

(ii) 3-SSG of G is not normal.

Q. $O(G)=39$ and G is non-abelian. How many normal subgroups in G?

Solution: $O(G)=3\times 13$, possible order of subgroups in G are 1,3,13 and 39.

Subgroups of G of order 1 and 39 are always normal ($H=\{e\}$ and $H=G$ are always normal)

13-SSG or order $13^1=13$ is unique
subgroup of G then 13-SSG is also normal subgroup of G.
If G is non-abelain then G has 13, 3-SSG then 3-SSG of order 3 is not normal subgroup of G.
Then,
Total No. of Normal subgroups in $G=1+1+1=3$.

Q. $O(G)=55$, how many subgroups in G?

(a) 4 (b) 14 (c) 16 (d) 2

Solution:

$O(G)=55=5\times 11,\ 5 \mid 11-1,$ then $\exists$ 2 possibilities

i.e.

$O(G)=55$ → Z_{55} / Non-abelian

(i) If G is abelian then G has exactly 4-subgroups

(ii) If G is non-abelain then G has 14 subgroups

Q. How many normal subgroups in G if $O(G)=55$.

(a) 4 (b) 3 (c) 14 (d) 2

Solution:

(i) If G is abelian then all subgroups are normal i.e. 4 normal subgroup

(ii) If G is non-abelian then exactly 3-normal subgroup

Q. If $O(G)=21$ and G is non-abelian then how many unique normal subgroup in G other than $\{e\}$ and G?

Ans. Unique

Q. $O(G)=168$ and G is simple, then how many 7-SSG in G?

(a) 1 (b) 7 (c) 8 (d) 28

Solution:

$O(G)=8\times3\times7$, $7^1 \mid O(G)$ but $7^{1+1}\times O(G)$ then G has 7-SSG of order $7^1=7$

# of 7-SSG in $G=1+7k, k=0,1,2,$ s.t. $1+7k \mid O(G)$

$n_7=1+7k=7$ is not possible for $k=0,1,2$

$n_7=1+7k=28$ is not possible for $k=0,1,2$

Since G is simple then G has only normal subgroup $\{e\}$ and G then has normal subgroup of order 1 and 168 only.

So,

$n_7=1+7k=1$, if $k=0$

then 7-SSG of order 7 is unique $\Rightarrow$ 7-SSG is normal subgroup of G but G is simple then $n_7=1$ is not possible $\Rightarrow n_7=1+7k=8$ is possible.

Q. $O(G)=77$, how many 7-SSG in G?

Solution:

$O(G)=7\times11$, here $7\times11-1$

$\therefore$ Unique 7-SSG exists in G

Above method can also be used.

Q. $O(G)=n$ and G is abelian, if G has 11-SSG, then how many?

Solution:

$O(G)=n$ and G is abelian then all the subgroups of G are normal. If G has 11-SSG then 11-SSG of G is normal subgroups of G.

Then, 11-SSG of G is unique.

Q. (i) $G=Z_2\times Z_4\times Z_4$, 2-SSG of G is normal?

(ii) How many 2-SSG in G?

Solution:

$O(G)=Z_2\times Z_4\times Z_4=32$, $2^5 \mid O(G)$ but $2^{5+1}\times 0$ then G has 2-SSG of order $2^5=32$.

Since G is abelian so 2-SSG is normal.

Hence, unique 2-SSG of G exists.

$G=Z_2\times Z_4\times Z_4$ is normal subgroup of G.

Q. $G=Z_2\times S_3$, 3-SSG is normal in G?

Solution:

$O(G)=O(Z_2\times S_3)=2\times6=12=2^2\times3$

$3^1 \mid O(G)$ but $3^{1+1}\times O(G)$ then G has 3-SSG of order

No of 3-SSG ${}^3G$

$n_3=1+3k,\ k=0,1,2,3,\ldots$ s.t. $1+3k \mid O(G)$

Put $k=0$, then $n_3=1+3\cdot0=1$ then $n_3=1$ is possible for 3-SSG.

Put $k=1$, then $n_3=4$ is possible for 3-SSG.

Then

#of 3-SSG in G is 1 or 4.

No. of subgroup of order 3 in $Z_2 \times S_3 = \dfrac{2}{\phi(3)} = \dfrac{2}{2} = 1$

then 3-SSG in G is unique.
$\therefore$ 3-SSG is normal in G.

Q. $G = Z_2 \times S_3$, 2-SSG of G is normal?

Solution:

$G = Z_2 \times S_3 = O(Z_2 \times S_3) = 12 = 2^2 \times 3$

$2^2 \mid O(G)$ but $2^{2+1} \times O(G)$ then G has 2-SSG of order 4.

$Z_2 \times S_3 = \{(0,I),(0,(12)),(0,(13)),(0,(23)),(0(123)),(0,(132)),(1,I),(1,(12)),(1,(13)),(1,(23)),(1,(123)),(1,(132))\}$

2-SSG of $Z_2 \times S_3$

$H_1 = \{(0,I),(0,(12)),(1,(12)),(1,I)\}$

$H_2 = \{(0,I),(0,(13)),(1,I),(1,(13))\}$

$H_3 = \{(0,I),(0,(23)),(1,I),(1,(23))\}$

Since 2-SSG of $Z_2 \times S_3$ is not unique then 2-SSG of $Z_2 \times S_3$ is not normal.

Verification: H_1 is not normal subgroup of $Z_2 \times S_3$

$x = (0,(123)) \in Z_2 \times S_3$

$h = (0,(12)) \in H_1$

$xhx^{-1} = (0,(123))(0,(12))(0,(123))^{-1}$

$= (0,(123))(0,(12))(0,(132))$

$= (0,(123))(12)(132)$

$= (0,(23)) \notin H_1$

then H_1 is not normal subgroup of $Z_2 \times S_3$.

Show that H_2 and H_3 also not normal subgroup of $Z_2 \times S_3$.

Q. 3-SSG of $S_3 \times S_3$ is normal in G?

Solution:

$O(G) = O(S_3 \times S_3) = O(S_3) \times O(S_3) = 6 \times 6 = 36 = 2^2 \times 3$

For 3-SSG, $3^2 \mid O(G)$ but $3^{2+1} \times O(G)$ then G has 3-SSG of order $3^2 = 9$

$G = S_3 \times S_3$ i.e. $G = G_1 \times G_2$

3-SSG of S_3 is normal

Similarly, 3-SSG of S_3 is normal.

Then, 3-SSG of $S_3 \times S_3$ is normal

$\therefore$ 3-SSG of $S_3 \times S_3$ is unique.

Note: p-SSG in $G_1 \times G_2 \times ..... \times G_n$ is normal if p-SSG is normal in each G_i.

Q. $G = Z_4 \times S_3$, 3-SSG of G is normal?
Solution:
3-SSG in Z_4 does not exist and 3-SSG in S_3 is normal then 3-SSG of $Z_4 \times S_3$ is normal.
Now, $O(Z_4 \times S_3) = O(Z_4) \times O(S_3) = 24 = 8 \times 3$
$3' | O(G)$ but $3^{1+1} \times O(G)$ then G has 3-SSG of order 3.
# of subgroup of order 3 in $Z_4 \times S_3 = \dfrac{2}{\phi(3)} = \dfrac{2}{2} = 1$
3-SSG of $Z_4 \times S_3 = \{(0, I), (0, (123)), (0, (132))\}$
Q. $G = Z_4 \times S_3$, subgroup of order 8 is normal subgroup in $Z_4 \times S_3$?
Solution:
$G = Z_4 \times S_3$
$O(G) = O(Z_4 \times S_3) = 2^3 \times 3$
For 2-SSG, $2^3 | O(G)$ but $2^{3+1} \times O(G)$ then G has 2-SSG of order $8 = 2^3$
Now, 2-SSG is normal in Z_4 but 2-SSG is not normal in S_3.
$\Rightarrow 2 - SSG$ is not normal in $Z_4 \times S_3$
Q. How many subgroup of order 8 in $Z_4 \times S_3$?
Q. $O(G) = 30$, then show that G is not simple.
Solution:
$O(G) = 30 = 2 \times 3 \times 5$
For 5-SSG, $5^1 | O(G)$ but $5^{1+1} \times O(G)$ then G has 5-SSG of order 5
# of 5-SSG in $G = 1 + 5k, k = 0, 1, 2, \ldots$ s.t. $1 + 5k | O(a)$
Put $k = 0$, then $n_5 = 1 + 5 \cdot 1 = 1$, $n_5 = 1$ is possible
Put $k = 1$, then $n_5 + 1 + 5 \cdot 1 = 6$, $n_5 = 6$ is possible
as $1 | O(G)$ and also $6 | O(G)$, hence $n_5 = 1$ and 6 is possible.
Similarly, $k = 2, 3, 4 \ldots$ are not possible for 5-SSG
then $n_5 = 1$ or $n_5 = 6$ ....(1)
For 3-SSG, $3^1 | O(G)$ but $3^{1+1} \times O(G)$ then G has 3-SSG of order 3
No. of 3-SSG in $G = 1 + 3k, k = 0, 1, 2$ s.t.l $1 + 3k | O(G)$
Put $k = 0$ then $n_3 = 1 + 3 \cdot 0 = 1$, $n_3 = 1$, $1 | O(G)$ then $n_3 = 1$ is possible.
Put $k = 0$, 1 and 2 not possible for 3-SSG then
Put $k = 3$, $n_3 = 1 + 3 \times 3 = 10$, $n_3 = 10$ and $10 | O(G)$ then $n_3 = 10$ is possible.
$\Rightarrow n_3 = 1$ or 10 ....(2)
From (1) and (2), 4 cases arises

	n_3	n_5
Case I	1	1

Case II	1	6
Case III	10	1
Case IV	10	6

Case I, II and III represent that G has normal subgroup other than $\{e\}$ and G then G is not simple and care IV is not possible for G.

In case IV, no. of elements of order 3 for each 3-SSG = 2

Total no. of elements of order 3 in G for 3-SSG

$=10\times 2=20$

Similarly, no. of elements for 5-SSG of order 5 = 4

Total no. of elements of order 5 in G for 5-SSG $=6\times 4=20$

Total No. of elements in G of order 3 and 5 = $20+24=44$

So case IV is not possible.

Note: up to Isomorphic = Non-isomorphic

Q. $O(G)=122$, how many non-isomorphic is possible.

Solution:

$O(G)=122=2\times 61,\ 2\,|\,61-1,\ \exists$ 2 possibility

$O(G)=122$ < Z_{122}, D_{61}

then 2 non-isomorphic group is possible

i.e. $G\approx Z_{122}$ or $G\approx D_{61}$

Note: $n=p_1^{r_1}\cdot p_2^{r_2}..........p_k^{r_k}$

then # of non-isomorphic abelian group of order n

$=P(r_1)\times P(r_2)\times........\times P(r_k)$

Q. $O(G)=24$, how many non-isomorphic abelian group?

Solution: $O(G)=24=2^3\times 3$

# of non-isomorphic abelian group $=P(3)\times P(1)$ = 3

(i) Z_{24} (ii) $Z_4\times Z_2\times Z_3$ (iii) $Z_2\times Z_2\times Z_2\times Z_2$

Q. $O(G)=10^5$, how many non-isomorphic abelian group?

Solution:

$O(G)=10^5=(2\times 5)^5=2^5\times 5^5$

# of non-isomorphic abelian group $=P(5)\times P(5)$

$=7\times 7=49$

[$H=\{e\}$ is trivial subgroup]

GROUP THEORY

1. GROUPS AND SUBGROUPS
2. CYCLIC GROUPS
3. COSETS, NORMAL SUBGROUPS & QUOTIENT GROUPS
4. HOMOMORPHISM AND AUTOMORPHISMS
5. PERMUTATION GROUPS

1. GROUPS AND SUBGROUPS

Q1. Let p be a prime number. Then show that

$(p-1)1+1 \equiv \mathrm{mod}(p)$

Also, find the remainder when $6^{44} \cdot (22)1+3$ is divided by 23.

Q2. If in the group G, $a^5 = e, aba^{-1} = b^2$ for some $a, b \in G$, find the order of b.

Q3. Prove that every group of order four is Abelian.

Q4. Let G be the set of all real numbers except -1 and define $a*b = a+b+ab \quad \forall a,b \in G$. Examine if G is an Abelian group under *.

Q5. Prove that the set of all bijective functions from a non-empty set X onto itself is a group with respect to usual composition of functions.

Q6. If G is a group in which $(a \cdot b)^4 = a^4 \cdot b^4, (a \cdot b)^5 = a^5 \cdot b^5$ and $(a \cdot b)^6 = a^6 \cdot b^6$ for all $a, b \in G$, then prove that G is Abelian.

Q7. Give an example of an infinite group in which every element has finite order.

Q8. Prove that if every element of a group $(G,0)$ be its own inverse, then it is an abelian group.

Q9. How many elements of order 2 are there in the group of order 16 generated by a and b such that the order of a is 8, the order of b is 2 and $bab^{-1} = a^{-1}$.

Q10. Show that the set

$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ of six transformations on the set of Complex numbers defined by

$f_1(z) = z,\ f_2(z) = 1 - z$

$f_3(z) = \frac{z}{(z-1)},\ f_4(z) = \frac{1}{z}$

$f_5(z) = \frac{1}{(1-z)}$ and $f_6(z) = \frac{(z-1)}{z}$ is a non-abelian group of order 6 w.r.t composition of mappings.

Q11. Let *a* and *b* be elements of a group with $a^2 = e$, $b^6 = e$ and $ab = b^4 a$. Find the order of ab, and express its inverse in each of the forms $a^m b^n$ and $b^m a^n$.

Q12. Let G be a group, and x and y be any two elements of G. IF $y^5 = e$ and $yxy^{-1} = x^2$, then show that $O(x) = 31$, where e is the identity element of G and $x \neq e$.

Q13. Let $G = \mathbf{R} - \{-1\}$ be the set of all real numbers omitting -1. Define the binary relation * on G by $a*b = a+b+ab$. Show $(G,*)$ is a group and it is abelian.

Q14. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} | a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is group under matrix multiplication.

Q15. Show that zero and unity are only idempotent of Z_n if $n = p^r$, where *p* is a prime.

2. CYCLIC GROUPS

Q1. Let G be a finite cyclic group of order *n*. Then prove that G has $\phi(n)$ generators (where ϕ is Euler's ϕ-function).

Q2. Let G be a finite group and let p be a prime. If p^m divides order of G, then show that G has a subgroup of order p^m, where m is a positive integer.

Q3. Let p be a prime number and z_p denote the additive group of integers modulo p. Show that every non-zero elements of z_p generates z_p.

Q4. Let G be a group of order pq, where p and q are prime numbers such that $p > q$ and $q \times (p-1)$. Then prove that G is cyclic.

Q5. How many generators are there of the cyclic group G of order 8? Explain. Taking a group $\{e, a, b, c\}$ of order 4, where e is the identity, construct composition tables showing that one is cyclic while the other is not.

Q6. If in a group G there is an element a of order 360, what is the order of a^{220}? Show that if G is a cyclic group of order n and m divides n, then G has a subgroup of order m.

Q7. Prove that a group of prime order is abelian. How many generators are there of the cyclic group $(G,\cdot)$ of order 8?

Q8. Given an example of group G in which every proper subgroup is cyclic but the group itself is not cyclic.

Q9. Let G be a group of order $2p, p$ prime. Show that either G is cyclic or G is generated by $\{a,b\}$ with relations $a^p = e = b^2$ and $bab = a^{-1}$.

Q10. Show that a cyclic group of order 6 is isomorphic to the product of a cyclic group of order 2 and a cyclic group of order 3. Can you generalize this? Justify.

Q11. Determine the number of homeomorphisms from the additive group z_{15} to the additive group z_{10} .(z_n is the cyclic group of order *n*).

3. COSETS, NORMAL SUBGROUPS & QUOTIENT GROUPS

Q1. Let G be a finite group, H and K subgroups of G such that $K \subset H$. Show that $(G:K)=(G:H)(H:K)$.

Q2. Write down all quotient groups of the group Z_{12}.

Q3. Prove that a non-commutative group of order $2n$, where n is an odd prime must have a subgroup of order n.

Q4. Let H be a cyclic subgroup of a group G. If H be a normal subgroup of G, prove that every subgroup of H is a normal subgroup of G.

Q5. Let H and K are finite normal subgroups of co-prime order of a group G. Prove that $hk = kh \forall h \in H$ and $k \in K$.

Q6. Let G be the set of all real 2×2 matrices $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, where $xz \neq 0$. Show that G is a group under matrix multiplication. Let N denote the subset $\left\{\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbf{R}\right\}$. Is N a normal subgroup of G? Justify your answer.

Q7. Prove that a non-empty subset H of a group G is normal subgroup of $G \Leftrightarrow$ for all $x, y \in H, g \in G, (gx)(gy)^{-1} \in H$.

Q8. If G is a finite Abelian group, then show that $O(a,b)$ is a divisor of l.c.m. of $O(a),O(b)$.

4. HOMOMORPHISM AND AUTOMORPHISMS

Q1. If G and H are finite groups whose orders are relatively prime, then prove that there is only one homomorphism from G to H, the trivial one.

Q2. Show that the quotient group of $(\mathbf{R},+)$ modulo $\mathbf{Z}$ is isomorphic to the multiplicative group of complex numbers on the unit circle in the complex plane. Here $\mathbf{R}$ is the set of real numbers and $\mathbf{Z}$ is the set of integers.

Q3. Find all the homeomorphisms from the group $(z,+)$ to $(z_4,+)$.

Q4. Show that the groups $z_5 \times z_7$ and z_{35} are isomorphic.

Q5. Let G be the group of non-zero complex numbers under multiplication, and let N be the set of complex numbers of absolute value 1. Show that G/N is isomorphic to the group of all positive real numbers under multiplication.

Q6. Let $(\mathbf{R}^*,\cdot)$ be the multiplicative group of non-zero reals and $(GL(n,\mathbf{R})X)$ be the multiplicative group of $n\times n$ non-singular real matrices. Show that the quotient group $GL(n,\mathbf{R})/SL(n,\mathbf{R})$ and $(\mathbf{R}^*,\cdot)$ are isomorphic where $SL(n,\mathbf{R})=\{A\in GL(n,\mathbf{R})/\det A=1\}$. What is the centre of GL $(n,\mathbf{R})$?

Q7. Prove or disprove that $(\mathbf{R},+)$ and $(\mathbf{R}^{+},\cdot)$ are isomorphic groups where $\mathbf{R}^{+}$ denotes the set of all positive real numbers.

Q8. If $\mathbf{R}$ is the set of real numbers and $\mathbf{R}_+$ is the set of positive real numbers, show that $\mathbf{R}$ under addition $(\mathbf{R},+)$ and $\mathbf{R}_+$ under multiplication $(\mathbf{R}_+,\cdot)$ are isomorphic. Similarly if $\mathbf{Q}$ is the set of rational numbers and $\mathbf{Q}_+$ the set of positive rational numbers are $(\mathbf{Q},+)$ and $(\mathbf{Q}_+,\cdot)$ isomorphic? Justify your answer.

5. PERMUTATION GROUPS

Q1. Let S_3 and Z_3 be permutation group on 3 symbols and group of residue classes module 3 respectively. Show that there is no homomorphism of S_3 in Z_3 except the trivial homomorphism.

Q2. Show that the smallest subgroup V of A_4 containing $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$ is isomorphic to the Klein 4-group.

Q3. Let G be a group of order *n*. Show that G is isomorphic to a subgroup of the permutation group s_n.

Q4. Show that any non-abelian group of order 6 is isomorphic to the symmetric group S_3.

Q5. What is the maximum possible order of a permutation in S_8, the group of permutations on the eight numbers $\{1,2,3,\ldots,8\}$? Justify your answer. (Majority of marks will be given for the justification.)

Q6. What are the orders of the following permutations in S_{10}?

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 7 & 3 & 10 & 5 & 4 & 2 & 6 & 9 \end{pmatrix}$ and $(1\ \ 2\ \ 3\ \ 4\ \ 5)(6\ \ 7)$.

Q7. What is the maximal possible order of an element in S_{10}? Why? Give an example of such an element. How many elements will there be in S_{10} of that order?

Q8. How many conjugacy classes does the permutation group S_5 of permutations 5 numbers have? Write down one element in each class (preferably in terms of cycles).

Q9. Show that in a symmetric group S_3, there are four elements σ satisfying $\sigma^2 =$Identity and three elements satisfying $\sigma^3 =$Identity.

Q10. Show that the alternating group on four letters A_4 has no subgroup of order 6.