Modern Algebra

M.Sc. Entrance

IIT-JAM | TIFR | DU | BHU | HCU | CMI | NBHM

Volume-II

MATHEMATICS-MA

CAREER ENDEAVOUR PUBLICATIONS has taken due care in collecting the data and providing the solutions, before publishing this book. Inspite of this, if any inaccuracy or printing errors are there, **CAREER ENDEAVOUR PUBLICATIONS** owes no responsibility. **CAREER ENDEAVOUR PUBLICATIONS** will be grateful if you could point out any such error. Your suggestions will be highly appreciated.

CAREER ENDEAVOUR Publications

Regd. Office: 28-A/11, Jia Sarai, New Delhi-16, **Ph:** 011-26851008, 26861009
E: info@cepublications.in, **W:** www.cepublications.in

Table of Content

Modern Algebra

Chapter 1

Number Theory Set Relation Function

Set: A well defined collection of distinct objects or things is called a set.
By well defined we mean that there is no confusion regarding inclusion or exclusion of any object.
Sets are usually denoted by capital letters $X, Y, Z.....$ whereas the objects collected in the set are called elements and denoted by small letters $x, y, z........$

Note: No set can be a member of itself.

Ex. (1) Let S_1 be the collection of first 5 natural numbers, then

$S_1 = \{1, 2, 3, 4, 5\}$

(2) S_2 be the collection of all Male human beings.
Then both S_1 and S_2 are sets.

Cardinality of Set :

The number of elements in a set is called the cardinality of the set. The cardinality of any set *A* is denoted by $|A|$.

Ex. $|S_1| = 5$ (in above example).

Subset :

A set *S* is called a subset of the set *T*, if each element of *S* is also an element of *T*. The symbols $\subset$ and $\subseteq$ are used for a subset; therefore $S \subset T$ or $S \subseteq T$.

Power Set :

Let *S* be any set. The collection of all subsets of *S* is called the power set of *S* and is denoted by *P*(*S*)

If $|S| = n$ then $|P(S)| = 2^{|S|} = 2^n$

Ex. Let $A = \{1, 2, 3\}$ then power set of *A* is

$P(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Clearly, *P* (*A*) contains 2^3 elements

Note: (*i*) The set without any element is called a null/void/empty set and is denoted by $\{\phi\}$. It is a subset of all the sets.

(*ii*) *P*(*S*), the power set, too includes ϕ. Hence *P*(*S*) is never empty (for any *S*), the cardinality of the power set is always some power of 2 if the set is finite.

Laws and Theorems for Union and Intersection of sets.

(I) Idempotent : For any A; $A \cup A = A$ and $A \cap A = A$

(II) Commutative : $A \cup B = B \cup A$ and $A \cap B = B \cap A$

(III) Associative : $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$

(IV) Identity Laws : ϕ is null set and *U* is a super set of *A*.

(*a*) $A \cup \phi = A$ (*b*) $A \cup U = U$ (*c*) $A \cap \phi = \phi$ (*d*) $A \cap U = A$

(V) Distributive Law : For any three sets *A*, *B* and *C*

(*a*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(*b*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(VI) Important Theorem : If $P(A)$ and $P(B)$ are the power sets of *A* and *B*.

(*a*) $P(A) \cap P(B) = P(A \cap B)$

(*b*) $P(A) \cup P(B) \subseteq P(A \cup B)$

(VII) De-Morgan's Law :

(*a*) $(A \cup B)' = A' \cap B'$

(*b*) $(A \cap B)' = A' \cup B'$

(*c*) $A - (B \cup C) = (A - B) \cap (A - C)$

(*d*) $A - (B \cap C) = (A - B) \cup (A - C)$

Some More Results

(*i*) $(A \cup B) \cap (A \cup B)' = \phi$

(*ii*) $(A - B) \cup (B - A) \cup (A \cap B) = A \cup B$

(*iii*) $A - (A - B) = A \cap B$

(*iv*) $A - B = B - A \Leftrightarrow A = B$

(*v*) $A \cup B = A \cap B \Leftrightarrow A = B$

(*vi*) $A \subseteq B \Leftrightarrow B' \subseteq A'$

(*vii*) $A - B = B' - A'$

Cartesian Product :

Let *X* and *Y* be sets. Then the set $X \times Y = \{(a, b) : a \in X, b \in Y\}$ is called the Cartesian product of *X* and *Y* and is a set of ordered pairs. If $|X| = n, |Y| = m$ then $|X \times Y| = m \cdot n$

Note: (*i*) $X \times Y \neq Y \times X$ [In general]

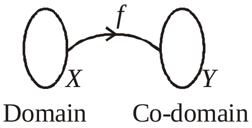
(*ii*) $X \times Y = Y \times X \Leftrightarrow \boxed{X = Y}$ ($\because$ *X* and *Y* are non empty sets).

(*iii*) If $X \cap Y = \phi \Rightarrow (X \times Y) \cap (Y \times X) = \phi$

(*iv*) If $|X \cap Y| = r \Rightarrow |(X \times Y) \cap (Y \times X)| = r^2$

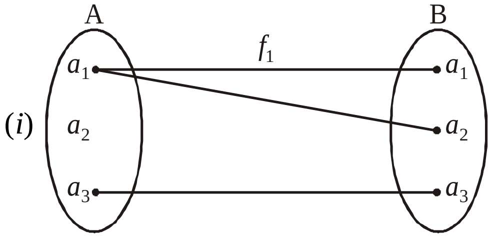
Functions (Mappings) and Relations

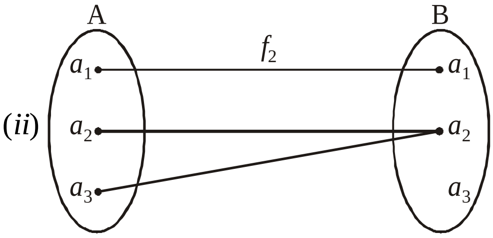
Function (Mapping): A function (or mapping) '*f* ' from a set '*X*' to a set '*Y*' is a rule which assigns to each element *x* of *X* exactly one element *y* of *Y*.

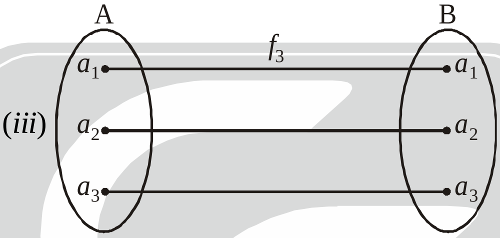


$'f : X \to Y'$

Example :--



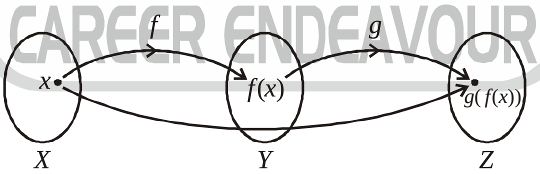




By the definition of a function that "a rule that assigns to each element x of X exactly one element y of Y", in above examples f_1 is not a function since a_1 maps to a_1 and a_2 both which contradicts the definition of a function, but f_2, f_3 ar clearly functions by defintion

Composition of Functions: Let $f : X \to Y$ and $g : Y \to Z$. The composition gof (or gf) is the mapping from X to Z defined by

$(gof)(x) = g(f(x))$ for all $x \in X$.



Example :

Let $f(x) = 2x$, $g(x) = x^2 + 1$

Then $fog(x) = f\left(g(x)\right) = f\left(x^2 + 1\right)$

$= 2 \cdot (x^2 + 1) = 2x^2 + 2$

but $gof(x) = g\left(f(x)\right) = g(2x)$

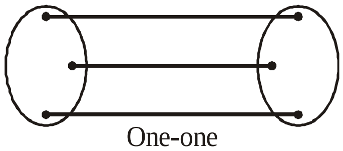
$\Rightarrow g(2x) = (2x)^2 + 1 = 4x^2 + 1$

Thus, $2x^2 + 2 \neq 4x^2 + 1$

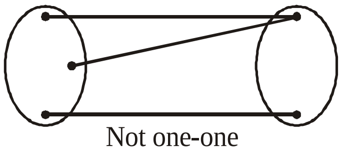
Hence composition of two functions need not be commutative. i.e., $fog(x) \neq gof(x)$.

One to one Function: A function $f : X \to Y$ is called one to one if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

or equivalently $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.



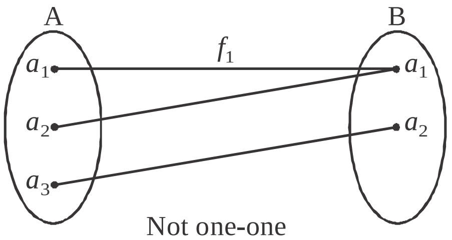
One-one



Not one-one

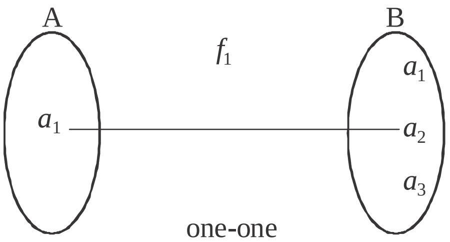
Example :

(*i*)



Not one-one

(*ii*)



one-one

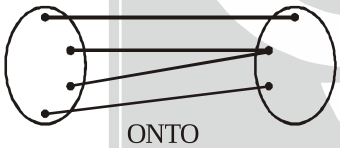
Remarks :

(*i*) If the domain has more elements than the codomain, then the function can not be one-one (by definition of a function)

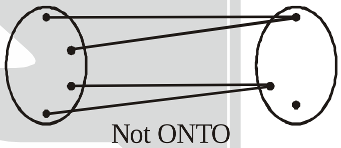
(*ii*) If domain has only one element then any function which is defined on that domain will always be one-one (by definition of a function)

(*iii*) If $|x| = m,\ |y| = n\,;\ m \leq n$ then number of one-one maps is ${}^nP_m = \dfrac{n!}{(n-m)!}$.

ONTO Functions: A function $f : X \to Y$ is said to be onto if each element of *Y* is the image of atleast one element of *X*.



ONTO



Not ONTO

Remarks :

(*i*) Similarly, if the codomain has more elements than the domain of a function, then the function can not be onto.

(*ii*) If the codomain of a function has only one element then it will always be onto which means for each $y \in Y, \exists$ at-least one $x \in X$ such that $f(x) = y$.

(*iii*) If $|x| = m,\ |y| = n\,;\ m \geq n,$ then the number of onto maps is

$$n^m - \left[\,{}^nC_1(n-1)^m - {}^nC_2(n-2)^m + {}^nC_3(n-3)^m - \cdots + (-1)^{k+1}\,{}^nC_k(n-k)^m\right]$$

Properties of Functions: Given functions $f : X \to Y, g : Y \to Z$ and $h : Z \to W$. Then

(i) $h(gf) = (hg)f$ (associativity)

(ii) If *f* and *g* are one-to-one, then *gof* and *fog* are one-to-one.

(iii) If *f* and *g* are onto, then *gof* and *fog* are onto.

(iv) If *f* is one-to-one and onto, then there exists a function f^{-1} from *Y* onto *X* such that

$(f^{-1}of)(x) = x\ \forall\, x \in X$ and $(fof^{-1})(y) = y\ \forall\, y \in Y$

Relation: Let A and B be two sets. A relation from A to B is a subset of $A \times B$ where $A \times B$ is the cartesian product of sets A and B i.e. $A \times B$ is a set of ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Example :

$A = \{1, 2, 3, 4\},\ B = \{a, b, c\}$. Then $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$. Then the power set of $A \times B$ is defined as the set of all relations on $A \times B$. Infact, each element of power set of $A \times B$ defines a relation and each relation defined on $A \times B$ gives a subset of $A \times B$.

$$\text{as } \mathbb{N} \times \mathbb{N} = \begin{cases} (1,1), & (1,2), \quad (1,3), \ldots \\ (2,1), & (2,2), \quad (2,3), \ldots \\ (3,1), & (3,2), \quad (3,3), \ldots \\ \quad | & \quad | \qquad\quad | \quad \ldots \\ \quad | & \quad | \qquad\quad | \quad \ldots \end{cases}$$

Then if we take all order pairs (a, b) s.t. $1 \le a \le 4$ and $b = 3$. Then $R = \{(1, 3), (2, 3), (3, 3), (4, 3)\}$ which is a subset of $\mathbb{N} \times \mathbb{N}$

Relation on a set *A*:

A relation on a set A is subset of $A \times A$.

Types of relations on a set:

(i) Reflexive Relation: Let R be a relation on a set A i.e. let R be a subset of $A \times A$, then R is called a reflexive relation if $(a, a) \in R, \forall a \in A$.

i.e. R is reflexive if we have, $aRa, \forall\, a \in A$

A relation R on a set A is NOT REFLEXIVE if there is atleast one element $a \in A$, such that $(a, a) \notin R$.

Example : (i) Reflexive : $A = \{1, 2, 3\}$

Then $R_1 = \{(1,1), (2, 2)\}$ ×

$R_2 = \{(1,1), (2, 2), (3, 3), (3, 4)\}$ √

$R_3 = \{(1,1), (2, 2), (3, 3)\}$ √

$R_4 = \{(1, 2), (2, 1), (2, 3), (3, 2), (1, 3), (3, 1)\}$ ×

R_1 and R_4 are not reflexive since they do not have all possible pairs $(a, a)\ \forall\ a \in A$.

R_2 and R_3 are reflexive since $\{(1,1), (2, 2), (3, 3)\} \subseteq R_3$

Similarly $\{(1, 1), (2, 2), (3, 3)\} \subseteq R_2$

(ii) Identity Relation: A subset I of $A \times A$ is called identity relation on A if $I = \{(a_1, a_1), (a_2, a_2), \ldots\ldots\ldots.(a_n, a_n)\} \subseteq A \times A$. On a set A, relation is said to be identity if every element of A is related to itself only. Identity relation is unique.

Note: Identity Relation is also Reflexive but not conversely.

Ex. $S = \{1, 2, 3\}$

$R = \{(1,1), (2, 2), (3, 3), (1, 2)\}$

is Reflexive but not identity relation.

(iii) Symmetric relation: Let R be a relation on a set A i.e. let R be a subset of $A \times A$. Then R is said to be a symmetric relation if $(a,b) \in R \Rightarrow (b,a) \in R$. Thus R is symmetric if we have bRa whenever we have aRb. A relation R on a set A is not symmetric if there exist two distinct elements $a, b \in A$, such that aRb but $b \not R a$.

i.e. $(a,b) \in R$ but $(b,a) \notin R$.

Example :

Set A = {1, 2, 3, 4}

$R_1 = \{(1,2), (2,1)\}$ √

$R_2 = \{(1,2), (1,3), (3,1), (4,4)\}$ ×

$R_3 = \{(1,1), (2,2), (3,3), (4,4)\}$ √

R_2 is not symmetric, since $(1,2) \in R_2$ but $(2,1) \notin R_2$

(iv) Anti-symmetric relation: Let R be a relation on a set A i.e. let R be a subset of $A \times A$. Then R is said to be an anti-symmetric relation if $(a,b) \in R$ and $(b,a) \in R$ implies $a = b$.

i.e. $(a,b) \in R$ and $(b,a) \in R \Rightarrow a = b$

if $a \neq b$ and $(a,b) \in R \Rightarrow (b,a) \notin R$

R is not anti-symmetric if there exist elements $a \neq b$ such that $(a,b) \in R$ as well as $(b,a) \in R$

(v) Transitive relation: Let R be a relation on a set A i.e. let R be a subset of $A \times A$. Then R is said to be a transitive relation if $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$. A relation R on a set A is not transitive if there exist elements a, b and c in A, not necessarily distinct, such that

$(a,b) \in R, (b,c) \in R$ but $(a,c) \notin R$

Example :

$A = \{1, 2, 3, 4\}$

$R_1 = \{(1,1), (2,2)\}$ √

$R_2 = \{(3,3), (3,4)\}$ √

$R_3 = \{(1,2), (2,1), (1,1)\}$ ×

R_1 and R_2 are transitive but R_3 is not since $(2,1) \in R_3$ and $(1,2) \in R_3$ but $(2,2) \notin R_3$.

Counting Techniques:

(a) Number of Relation on a set :

Let A be a set such that $|A| = n$ then we consider $A \times A$, then every subset of $A \times A$ is a relation then total number of relations on $A = |P(A \times A)| = 2^{n^2}$

(b) Total number of Reflexive relation on $A = 2^{n^2 - n}$

Ex. Number of reflexive relations on a set $A = \{1, 2, 3, 4\}$ is $2^{4^2 - 4} = 2^{16-4} = 2^{12}$ ← Ans.

(c) Number of SYMMETRIC relation on $A = 2^{\sum n}$

(d) Number of ANTI-SYMMETRIC relations = $2^n \cdot 3^{\sum (n-1)}$

Equivalence Relation: Let R be a relation on a set A. Then R is said to be an equivalence relation iff the following three conditions hold simultaneously.

(i) R is reflexive i.e. $a \in A \Rightarrow (a,a) \in R$

(ii) R is symmetric i.e. $(a,b) \in R \Rightarrow (b,a) \in R$

(iii) R is transitive i.e. $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$

Ex. (*i*) Set of parallel lines.

(a) Reflexive:- Each line is parallel to itself.

(b) Symmetric:- If $L_1 \parallel L_2$ then $L_2 \parallel L_1$. Hence symmetric hold.

(c) Transitivity:- If $L_1 \parallel L_2$ and $L_2 \parallel L_3 \Rightarrow L_1 \parallel L_3$. Hence set of parallel lines defines an equivalence relation.

Ex. (*ii*) Set of all male human being with relation defined as brotherhood :-

(a) Reflexivity :- Each male human being is brother of himself.

(b) Symmetric :- If A_1 is brother of A_2 then A_2 is also brother of A_1. (Since we have the set of all male human being).

(c) Transitive :- Also holds. Hence an equivalence relation.

1. The relation "congruence modulo *m*" is an equivalence relation. As,

(I) $a - a = 0$

Then $m|0$, so, $a\ R\ a\ \forall a$ (Reflexive)

(II) If $a\ R\ b$

$\Rightarrow a \equiv b \,(\text{mod } m)$

$\Rightarrow m|(a-b) \;\Rightarrow m|-(b-a) \;\Rightarrow m|(b-a)$

$\Rightarrow b \equiv a\,(\text{mod } m)$ and so $b\ R\ a$ (symmetry)

(III) If $a\ R\,b,\ b\ R\ c$

$\Rightarrow m|(a-b)$ and $m|(b-c)$

$\Rightarrow m\left|\left(a-\cancel{b}+\cancel{b}-c\right)\right. \;\Rightarrow\; m|(a-c)$

$\Rightarrow a\ R\,c$ (Transitivity)

Hence " congruence modulo *m*" is an equivalence relation.

2. Let $\mathbb{R}$ be a set of real numbers then $a\ R\ b \Leftrightarrow |a-b| \geq 0$. Relation R is an equivalence relation.

(*i*) Reflexivity :-- $|a-a| = 0\ \forall\ a \in \mathbb{R}$

$\therefore a\ R\ a$

(*ii*) Symmetry :-- If $a\ R\ b \Rightarrow |a-b| \geq 0$

$\Rightarrow |b-a| \geq 0 \Rightarrow b\ R\ a$

(*iii*) Transitivity :-- If $a\ R\ b$ and $b\ R\ c$

$\Rightarrow |a-b| \geq 0,\ \ |b-c| \geq 0$

$\Rightarrow |a-b+b-c| = |a-c| \geq 0$

$\Rightarrow a\ R\ c$

Examples: which is not an equivalence relation.

(i) set of perpendicular lines

(a) not reflexive as a line cannot be perpendicular to itself.

(b) it is symmetric

(c) not transitive

Hence not an equivalence relation.

Equivalence Class: If $\sim$ is an equivalence relation on a set A and $a \in A$, then the set $[a] = \{x \in A : x \sim a\}$ is called the equivalence class of A containing 'a'.

$[a]$ is a subset of A.

Properties of Equivalence Classes: Let A be a non-empty set and let R be an equivalence relation on A. Let a and b be arbitrary elements of A. Then

(i) $a \in [a]$

(ii) If $b \in [a]$, then $[b] = [a]$

(iii) $[a] = [b]$ iff aRb i.e. $(a,b) \in R$

(iv) Either $[a] = [b]$ or $[a] \bigcap [b] = \phi$ i.e. two equivalence classes are either disjoint or identical.

Proof: (i) Since R is reflexive, we have aRa. But $[a] = \{x \mid x \in A \text{ and } xRa\}$. Now, $a \in A$ and aRa imply $a \in [a]$.

(ii) Let $b \in [a] \Rightarrow bRa$. Now if, x be any arbitrary element of [b]. Then $x \in [b] \Rightarrow xRb$. But R is transitive, therefore xRb and $bRa \Rightarrow xRa$ $\Rightarrow x \in [a]$. Thus if $x \in [b] \Rightarrow x \in [a]$. Therefore $[b] \subseteq [a]$. Again, let y be any arbitrary element of [a]. Then $y \in [a] \Rightarrow yRa$.

Since R is symmetric, therefore $bRa \Rightarrow aRb$. Now yRa and $aRb \Rightarrow yRb$ $\Rightarrow y \in [b]$

Thus if $y \in [a] \Rightarrow y \in [b]$. Therefore $[a] \subseteq [b]$. Finally $[a] \subseteq [b]$ and $[b] \subseteq [a] \Rightarrow [a] = [b]$

(iii) **First Part:** Suppose we have given $[a] = [b]$ and we have to prove aRb

Since R is reflexive, therefore we have aRa.

Now $aRa \Rightarrow a \in [a] \Rightarrow a \in [b]$ $[\because [a] = [b]]$ $\Rightarrow aRb$

Thus if $[a]=[b] \Rightarrow aRb$

Converse part: Suppose that aRb, then to prove that $[a] = [b]$.

Let x be any arbitrary element of [a]. Then xRa. But it is given that aRb.

Therefore, xRa and $aRb \Rightarrow xRb$ [R is transitive]

$\Rightarrow x \in [b]$

Thus if $x \in [a] \Rightarrow x \in [b]$. Therefore $[a] \subseteq [b]$

Similarly $[b] \subseteq [a]$

$\Rightarrow [a] = [b]$

Therefore, $[a] = [b]$ iff aRb

(iv) If $[a] \bigcap [b] = \phi$, then we have nothing to prove. So let us suppose that $[a] \bigcap [b] \neq \phi$ therefore there exist an element $x \in A$ such that $x \in [a] \bigcap [b]$

$\Rightarrow x \in [a]$ and $x \in [b]$

$\Rightarrow xRa$ and xRb

$\Rightarrow aRx$ and xRb [R is symmetric]

$\Rightarrow aRb$ [R is transitive]

$\Rightarrow [a]=[b]$

Thus if $[a]\cap[b]\neq\phi \Rightarrow [a]=[b]$

Partition: A partition of a set *S* is a collection of non-empty disjoint subsets of *S* whose union is *S*.

Example 1: Consider the set $S=\{1,2,3,4\}$, then $\{\{1,2\},\{3\},\{4\}\}$ is a partition of *S*.

Example 2: Let $\mathbb{Z}$ be the set of all integers. We know that $x\equiv y(\bmod 3)$ is an equivalence relation on $\mathbb{Z}$. Consider the set of three equivalence classes

$[0]=\{....,-6,-3,0,3,6,.....\}$, $[1]=\{....,-5,-2,1,4,7,.....\}$, $[2]=\{....,-4,-1,2,5,8,.....\}$

We observe that

(i) The sets [0], [1] and [2] are non-empty

(ii) The sets [0], [1] and [2] are pairwise disjoint

(iii) $\mathbb{Z}=[0]\cup[1]\cup[2]$

Hence, $\{[0],[1],[2]\}$ is a partition of $\mathbb{Z}$, under the relation $x\equiv y\ (\bmod 3)$.

Relation induced by a partition of a set: Corresponding to any partition of a set *S*, we can define a relation *R* on *S* by the requirement that xRy iff *x* and *y* belong to the same subset of *S* belonging to the partition. The relation *R* is then said to be induced by the partition.

Example 1 : Consider the set $S=\{1,2,...9,10\}$ and its subsets

$B_1=\{1,3\}, B_2=\{7,8,10\}, B_3=\{2,5,6\}, B_4=\{4,9\}$.

The set $p=\{B_1,B_2,B_3,B_4\}$ is such that

(i) B_1,B_2,B_3,B_4 are all non-empty subsets of *S*.

(ii) $B_1\cup B_2\cup B_3\cup B_4=S$, and

(iii) For any sets B_i, either $B_i=B_j$ or $B_i\cap B_j=\phi$.

Hence the set $\{B_1,B_2,B_3,B_4\}$ is a partition of *S*.

Fundamental theorem on equivalence relation: An equivalence relation *R* on a non-empty set *S* determines a partition of *S* and conversely a partition of *S* defines an equivalence relation on *S*. OR

The equivalence classes of an equivalence relation on a set *S* constitute a partition of *S* conversely, for any partition *P* of *S*, there is an equivalence relation on *S* whose equivalence classes are the elements of *P*.

Concept of Divisibility: A non-zero integer '*t*' is said to be a divisor of an integer '*s*' if there is an integer *u* such that $s=tu$. In this case we write *t*|*s*.

Example :

(*i*) 6|12 as 12 can be written as 12 = 6.2

So 6 divides 12

(*ii*) $5\nmid 7$, since there is no *u*, s.t. 7 = 5*u*. Hence 5 does not divides 7.

Prime Number : A prime number is a positive integer greater than 1 whose only positive divisors are 1 and itself. e.g. 17, 13, 11 etc.

Division Algorithm : Let '*a*' and '*b*' are integers with *b* > 0. Then there exist unique integer *q* and *r* with the property that $a=bq+r$ where $0\le r<b$, *q* is called the quotient and *r* is remainder.

e.g. for *a* = 17 and *b* = 5

Division algorithm gives 17 = 5. 3 + 2

For a = –23, b = 6

We have –23 = 6(–4) + 1

G.C.D. (Greatest Common Divisor): The greatest common divisor of two non-zero integers 'a' and 'b' is the largest of all common divisors of a and b. We denote this integer by gcd(a, b) or (a, b)

Remarks : If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Example :

(i) gcd (5, 12) = 1, since '1' is the only number which divides 5 and 12 both.

(ii) gcd (4, 12) = 4 is greatest common divisor as 4|4 and 4|12

(iii) gcd (10, 25) = 5 as 5|10 and 5|25 and there is no other divisor of both 10 and 25 which is >5

Relatively Prime Integers or Coprime integer : When $\gcd(a,b)=1$, we say a and b are relatively prime or coprime integers

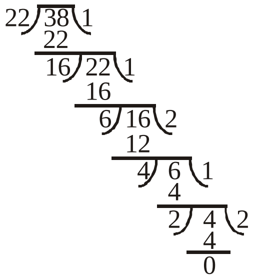
e.g. $\gcd(9,10)=1, \gcd(5,8)=1$

Example :

gcd (10, 20) = 10 as 10 is the greatest common divisor of (10, 20) so, they are not relatively prime.

Composite number: which are not prime numbers and 1 i.e. (other than prime number and 1 all integers are composite)

e.g. To compute $\gcd(a,b)$ by Euclidean Algorithm. Exp: To compute $\gcd(38,22)$



38 = 22.1 + 16
22 = 16.1 + 6
16 = 6.2 + 4
6 = 4.1 + 2
4 = $\boxed{2}$.2 + 0
$\downarrow$
gcd(38, 22)

gcd(2520, 154)

2520 = 154.16 + 56
154 = 56.2 + 42
56 = 42.1 + 14
42 = $\boxed{14}$.3 + 0
$\downarrow$
gcd(2520, 154)

Euclid's Lemma: If p is a prime number that divides $a.b$, then either p divides a or p divides b.

$\boxed{\text{i.e. } p \mid ab \Rightarrow \text{either } p \mid a \text{ or } p \mid b}$

Exp. $3 \mid 12 \Rightarrow 3 \mid 4.3 \Rightarrow 3 \mid 3$

When p is not a prime, then Euclid's Lemma may fail.

$6 \mid 4.3$ but $6 \nmid 4$ and $6 \nmid 3$

Fundamental Theorem of Arithmetic: Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. Thus, if $n = p_1 p_2 .....p_r$ and $n = q_1 q_2 .....q_s$ where p's and q's are primes, then $r = s$ and, after re-numbering the q's, we have $p_i = q_i$ for all i.

Example :

(i) 30 = 2 × 3 × 5, Thus, $p_1 = 2,\ p_2 = 3,\ p_3 = 5$

(ii) 15 = 3 × 5, $p_1 = 3,\ p_2 = 5$

(iii) 42 = 2 × 3 × 7, $p_1 = 2,\ p_2 = 3,\ p_3 = 7$

These expressions are unique. No other primes exist other than these which gives same number in each example given above.

Least Common Multiple: lcm (a, b): The least common multiple of two non-zero integers a and b is the smallest positive integer that is a multiple of both a and b. e.g. lcm(4, 6) = 12

Example :

(*i*) $lcm\ (5, 8) = 40$ (*ii*) $lcm\ (10, 20) = 20$

Remarks : $a \cdot b = \text{lcm}(a, b).\text{gcd}(a, b)$, so, if $gcd\ (a, b) = 1$, then $lcm\ (a, b) = a \cdot b$.

■ If $a \mid m$ and $b \mid m$ then $l \mid m$ [where l is lcm (a, b).

Modular Arithmetic: Modular arithmetic is an abstraction of a method of counting that you often use. for example, if it is now January, what will be 25th month from now? of course February.

25 = 12.2 + 1, when $a = nq + r$, where q is the quotient and r is the remainder upon dividing a by n, we write

$a \bmod n = r$ or $a \equiv r \bmod n$

Thus $3 \bmod 2 = 1$ since $3 = 2.1 + 1$, $6 \bmod 2 = 0$ since $6 = 2.3 + 0$

$62 \bmod 85 = 62$ since $62 = 85.0 + 62$

More generally, if a and b are integers and n is a positive integer, we often write $a \equiv b \bmod n$ whenever $n \mid (a - b)$.

$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$, $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

$(17 + 23) \bmod 10 = ((17 \bmod 10) + (23 \bmod 10)) \bmod 10 = (7 + 3) \bmod 10 = 10 \bmod 10 = 0$

Example :

$12 \equiv -2 \bmod (7)$ means $7 \mid 12 - (-2) \Rightarrow 7 \mid 14$

Some properties of modular Arithmetic

If $a \equiv b$ (mod n), then

(*i*) $a + c \equiv b + c$ (mod n)

(*ii*) $a\,c \equiv b\,c$ (mod n)

(*iii*) $a^p \equiv b^p$ (mod n)

(*iv*) $p(a) \equiv p(b)$ (mod n)

where $p(a)$ polynomial in a.

but converse of the property (ii), (iii) and (iv) does not hold.

as, $9 \equiv 6 \bmod (3)$

also $3.3 \equiv 3.2 \bmod (3)$

but $3 \equiv 2 \bmod (3)$ not hold

Similarly for others.

SOME IMPORTANT FUNCTIONS

1. ϕ **– function :** It is called Euler phi-function and is defined as the function ϕ: N→ N such that and $\phi\ (1) = 1$, $\phi(n)$ = number of positive integers co-prime to n and less than or equal to n.

Ex. (*i*) $\phi(10) = 4$ as 1, 3, 7, 9 (total 4) integers which are co-prime to 10.

Method for finding number of positive integers co-prime to n :--

If $n = p^a\ q^b \cdot r^c, \ldots$ where $p, q, r, \ldots$ are prime and $a, b, c, \ldots$ are natural number.

Then $\phi(n) = n \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right) \ldots$

or $\phi(n) = (p^a - p^{a-1})(q^b - q^{b-1})(r^c - r^{c-1})\ldots$

Ex. (*ii*) $\phi(100) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$

$$= 5^2 \cdot 2^2 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right)$$
$$= 2 \cdot 5\,(1) \cdot (4)$$
$$= 40$$

or $\phi(100) = (2^2 - 2^{2-1})(5^2 - 5^{2-1})$

$$= (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$$

2. **$\tau(n)$: (τ (tau) function)**:-- It gives the total number of positive divisors of *n*, including 1 and *n* both.

If $n = p^a \cdot q^b \cdot r^c, \ldots$ where $p, q, r, \ldots$ are distinct primes and $a, b, c \ldots \in \mathbb{N}$. Then $\tau : N \to N$ define as

$\tau(n) = (a+1)\,(b+1)\,(c+1)\ldots$

Note: It includes 1 and and the number itself.

$\tau(100) = \tau(2^2 \cdot 5^2) = (2+1)\,(2+1) = (3)\,(3) = 9$

(*iii*) $\sigma(n)$:-- (Sigma function) :-- It gives the sum of all positive divisors of *n*. It too includes 1 and the number *n* itself.

If $n = p^a \cdot q^b \cdot r^c$..........., p, q, r primes $a, b, c \in \mathbb{N}$.

Then $\sigma(n) = \left(\frac{p^{a+1} - 1}{p - 1}\right) \cdot \left(\frac{q^{b+1} - 1}{q - 1}\right) \cdot \left(\frac{r^{c+1} - 1}{r - 1}\right)$............

Ex. $\sigma(20) = \sigma\left(2^2 \cdot 5\right) = \left(\frac{2^3 - 1}{1}\right) \cdot \left(\frac{5^2 - 1}{4}\right) = (7) \times \left(\frac{24}{2}\right) = 7 \times 6 = 42$

Properties :

1. In particular when *n* is prime say *p*,

$\phi(p) = p - 1, \tau(p) = 2, \sigma(p) = p + 1$

2. If gcd (*m*, *n*) = 1 then

(*i*) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

(*ii*) $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$

(*iii*) $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$

3. A “number theoretic” function *f* is said to be multiplicative if $f(m \cdot n) = f(m) \cdot f(n)$. Whenever g.c.d. (*m*, *n*) = 1 hence ϕ, τ, σ are multiplicative functions.

4. For *n* > 2, $\phi(n)$ is always an even integer.

5. $\phi(10^n) = 4 \times 10^{n-1}$

Important Theorems :

(I) Gauss : For each positive integer $n \geq 1$.

$\boxed{n = \sum_{d|n} \phi(d)}$ where sum is being extended over all positive divisors ‘*d*’ of *n*.

(II) Theorem : For $n > 1$, the sum of the positive integers less than n and relatively prime to n is

$$\boxed{\sum_{\substack{(K,n)=1\\ 1\le K\le n}} K = \frac{1}{2} n\cdot\phi(n)}$$

(III) Fermat's Theorem : If p is prime, then $a^p \equiv a \,(\text{mod } p)$.

(IV) Fermat's little Theorem : If p is prime, then $a^{p-1} \equiv 1(\text{mod } p)$
converse of Fermat's theorem is need not to be true.

(V) Euler's Theorem : If n is a positive integer and g.c.d. $(a, n) = 1$, then $a^{\phi(n)} \equiv 1\,(\text{mod } n)$, $\phi(n)$ is Euler phi function "Euler Theorem is generalization of Fermat's Theorem". OR

$$\#\begin{bmatrix}\text{i.e. if } x^k \equiv a \,(\text{mod } n) \text{ and } \gcd(k,\phi(n)) = d \text{ ; } n \text{ is prime}\\ \Leftrightarrow a^{\phi(n)/d} \equiv 1(\text{mod } n), \text{where } \phi(n) \text{ is Euler } \phi \text{ function}\end{bmatrix}$$

(VI) Wilson's Theorem : If p is a prime, then $(p-1)! \equiv -1\,(\text{mod } p)$ or $(p-1)!+1 \equiv 0\,(\text{mod } p)$.

(VII) Pseudo Prime : A composite integer 'n' is called pseudo prime if it satisfies the congruence equations. $2^n \equiv 2\,(\text{mod } n)$.

(VIII) Chinese Remainder Theorem

Let $x \equiv a_i \text{ mod } m_i : i = 1,\ldots,n$, for which m_i are pairwise relatively prime then the solution of the set of congruence is $x = \left(a_1 b_1 \dfrac{m}{m_1} + \cdots a_n b_n \dfrac{m}{m_n}\right) \text{mod } m$, where $m = m_1 m_2 \ldots m_n$ and b_i satisfy $b_i \dfrac{m}{m_i} = 1\,(\text{mod } m_i)$

If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers and if $a_1, a_2, \ldots, a_n$ are any integers then simultaneous congruence $x = a_i \text{ mod } m_i \text{ ; } i = 1,\ldots,n$ have a solution and solution is unique modulo m, where $m = m_1 m_2 \ldots m_n$.

Solved Examples

1. Let a relation R be defined over the set of rational numbers Q by $a\,R\,b$ if $a > b$. Then this relation is

(a) reflexive, but not symmetric and transitive (b) symmetric, but not reflexive and transitive **[B.H.U-2011]**

(c) transitive, but not reflexive and symmetric (d) not transitive, but reflexive and symmetric

Soln. Given a relation over the set of rational numbers $\mathbb{Q}$ by $a\text{R}b$ if $a > b$

Now $a \not> a \Rightarrow R$ is not reflexive

Also if $a > b$ then $a \not< b$

$\Rightarrow R$ is not symmetric

Let $a,b,c \in \mathbb{Q}$ be such that $a > b$ and $b > c$

$\Rightarrow a > c$

$\Rightarrow R$ is transitive

Hence correct option is (c)

2. Which of the following is not an equivalence relation ?

(a) The relation R defined on $\mathbb{N}\times\mathbb{N}$ by $(a,b)\,R\,(c,d)$ if $a+d=b+c$

(b) The relation of 'brotherhood' over the set of men

(c) The relation R defined over the set of non-zero rational numbers by $a\,R\,b$ if $ab=1$

(d) The relation R defined over the set of integers by $a\,R\,b$ if $a-b$ is divisible by 7

Soln. Clearly (a), (b) and (d) are equivalence relations

for option (c)

Let $a = 2$

$aa = 4 \neq 1$

$\Rightarrow$ Given relation is not reflexive

Thus it is not an equivalence relation

Hence correct option is (c)

3. Let a relation R be defined on the set of complex numbers $\mathbb{C}$ by ZRW to mean $\operatorname{Re}(Z)\leq\operatorname{Re}(W)$ and $\operatorname{Im}(Z)\leq\operatorname{Im}(W)$. Then this relation R is

(a) reflexive and transitive but not symmetric (b) symmetric and transitive but not reflexive

(c) reflexive and symmetric but not transitive (d) symmetric but not reflexive and transitive

Soln. Let $Z, W, V \in \mathbb{C}$

Clearly $\operatorname{Re}(Z)\leq Re(Z)$ and $\operatorname{Im}(Z)\leq\operatorname{Im}(Z)$

$\Rightarrow ZRZ$

$\Rightarrow R$ is reflexive

Let $Z=1+2i$ and $W=3+4i$

Clearly $\operatorname{Re}(Z)\leq\operatorname{Re}(W)$ and $\operatorname{Im}(Z)\leq\operatorname{Im}(W)$

$\Rightarrow ZRW$

But $Re(W)\not\leq\operatorname{Re}(Z)$ and $\operatorname{Im}(W)\not\leq\operatorname{Im}(Z)$

$\Rightarrow W\not R Z$

$\Rightarrow R$ is not symmetric

Clearly R is transitive

Hence correct option is (a)

4. Remainder of 8^{103} from Fermat theorem when divided by 103 is

(a) 8 (b) 7 (c) 6 (d) 10

Soln. By Fermat theorem, we have

$8^{103}\equiv 8\pmod{103}$

Thus remainder is 8

Hence correct option is (a)

5. The remainder when 7^{1000} is divided by 24 is :

(a) 1 (b) 3 (c) 5 (d) 7

Soln. $7^2 \equiv 1(\text{mod } 24)$

$\Rightarrow (7^2)^{500} \equiv 1^{500}(\text{mod } 24)$

$\Rightarrow 7^{1000} \equiv 1(\text{mod } 24)$

Hence correct option is (a)

6. The remainder of $(37)^{49}$ when divided by 7 is

(a) 3 (b) 1 (c) 2 (d) 6

Soln. $37 \equiv 2(\text{mod } 7)$

$\Rightarrow (37)^2 \equiv 2^2(\text{mod } 7)$

$\Rightarrow (37)^3 \equiv 2^3(\text{mod } 7) \equiv 1(\text{mod } 7)$

$\Rightarrow \left((37)^3\right)^{16} \equiv 1^{16}(\text{mod } 7)$

$\Rightarrow (37)^{48} \equiv 1(\text{mod } 7)$

$\Rightarrow (37)^{49} \equiv 2(\text{mod } 7)$

Hence correct option is (c)

7. The smallest positive integer n such that $5^n - 1$ is divisible by 36 is

(a) 2 (b) 3 (c) 5 (d) 6

Soln. $5^2 \equiv 25(\text{mod } 36)$

$\Rightarrow 5^3 \equiv 17(\text{mod } 36)$

$\Rightarrow 5^4 \equiv 85(\text{mod } 36) \equiv 13(\text{mod } 36)$

$\Rightarrow 5^5 \equiv 65(\text{mod } 36) \equiv 29(\text{mod } 36)$

$\Rightarrow 5^6 \equiv 145(\text{mod } 36)$

$\Rightarrow 5^6 \equiv 1(\text{mod } 36)$

Hence correct option is (d)

8. Let X be the set of all non-empty finite subsets of $\mathbb{N}$. Which one of the following is not an equivalence relation on X: **[HCU-2011]**

(a) $A \sim B$ if and only if min A = min B

(b) $A \sim B$ if and only if A, B have same number of elements

(c) $A \sim B$ if and only if $A = B$

(d) $A \sim B$ if and only if $A \cap B = \phi$

Soln. Clearly (a), (b) and (c) are equivalence relations

For option (d)

Let $A=\{1,2\}, B=\{3,4\}, C=\{2,5\}$

Clearly $A\cap B=\phi$ and $B\cap C=\phi$

But $A\cap C\neq\phi$

Thus given relation is not transitive

$\Rightarrow$ This relation is not an equivalence relation

Hence correct option is (d)

9. If n and m are positive integers and $n^9=19m+r$, then the possible values for r modulo 19 are

(a) only 0 (b) only $0, \pm1$ (c) only ±1 (d) None of the above **[TIFR-2010]**

Soln. By Fermat's theorem, we have

$$n^{18}\equiv1(\text{mod}19)$$

$$\Rightarrow19\,|\left(n^{18}-1\right)$$

$$\Rightarrow19\,|\left(\left(n^9-1\right)\left(n^9+1\right)\right)$$

Now 19 is a prime number

$\Rightarrow$ Either $19\,|\left(n^9-1\right)$ or $19\,|\left(n^9+1\right)$

If $19\,|\left(n^9-1\right)\Rightarrow n^9\equiv1(\text{mod}\,19)$

$\Rightarrow$ Remainder is 1

If $19\,|\left(n^9+1\right)\Rightarrow n^9\equiv-1(\text{mod}\,19)$

$\Rightarrow$ Remainder is -1

Hence correct option is (c)

10. Write down the last two digits of 9^{1500}. **[NBHM-2007]**

Soln. Since $(9,100)=1$

and $3^2\equiv9(\text{mod}100)$, then by Euler's theorem

$$9^{\phi(100)/2}\equiv1(\text{mod}100)$$

$$\Rightarrow9^{40/2}\equiv1(\text{mod}100)$$

$$\Rightarrow9^{20}\equiv1(\text{mod}100)$$

$$\Rightarrow\left(9^{20}\right)^{75}\equiv1^{75}(\text{mod}100)$$

$$\Rightarrow9^{1500}\equiv1(\text{mod}100)$$

Hence last two digit is (1)

11. If n is not a multiple of 23 then the remainder when n^{11} is divided by 23 is $\pm 1 (\text{mod } 23)$. **[TIFR-2012]**

Soln. By Fermat theorem, we have

$$n^{23-1} \equiv 1 (\text{mod } 23)$$

$$\Rightarrow n^{22} \equiv 1 (\text{mod } 23)$$

$$\Rightarrow 23 | (n^{22} - 1)$$

$$\Rightarrow 23 | (n^{11} - 1)(n^{11} + 1)$$

$\Rightarrow$ Either $23 | (n^{11} - 1)$ or $23 | (n^{11} + 1)$

$\Rightarrow$ Either $n^{11} \equiv 1 (\text{mod } 23)$ or $n^{11} \equiv -1 (\text{mod } 23)$

$$\Rightarrow n^{11} \equiv \pm 1 (\text{mod } 23)$$

Hence given statement is true

12. There exists a subset A of $\mathbb{N}$ with exactly five elements such that the sum of any three elements of A is a prime number. **[TIFR-2017]**

Soln. It is not possible for such a set to exist when a number is divided by 3, it can leave 3 possible remainders 0, 1 and 2. If 3 numbers in the set leave the same remainder when divided by 3, then their sum would be divisible by 3. So, this number is composite.

So, for this set to be exist, no more than 2 elements can have the same remainder.

Case-I: When remainder is 0, 0, 1, 1 2. Now 0+1+2 is divisible by 3

$\Rightarrow$ This number is composite

Case-II: when remainder is 0,0, 1, 2, 2. Now 0 +1+2 is divisible by 3.

$\Rightarrow$ This number is composite

Hence this set does not exist

Hence given state is false.

13. What is the smallest positive positive integer in the set $\{24x + 60y + 2000z \mid x, y, z \in \mathbb{Z}\}$

(a) 2 (b) 4 (c) 6 (d) 24

Soln. $\gcd(24, 60, 2000) = 4$

Hence, correct option is (b).

14. True or False

The equation $63x + 70y + 15z = 2010$ has an integral solution **[TIFR-2011]**

Soln. By definition of $\gcd(63, 70, 15)$ there exist $x, y, z \in \mathbb{Z}$ such that $1 = \gcd(63, 70, 15) = 63x + 70y + 15z$,

$$\text{then} \begin{array}{rcl} 2010 &=& 63(2010x) + 70(2010y) + 15(2010z) \\ 2010 &=& 63x' + 70y' + 15z' \end{array}$$

So we get x', y', z' are integral solution of the equation.

Hence this is true statement.

15. **True or False**

Given any integer $n \geq 2$ we can always find an integer m such that each of $n-1$ consecutive integers $m+2$, $m+3, \ldots, m+n$ are composite. **[TIFR-2012]**

Ans. True

Soln. Take $m = \text{lcm}\,\{2, 3, 4, \ldots, n\}$, Then $m+2$, $m+3, \ldots\ldots\ldots, m+n$ are composite

16. The last digit of 2^{80} is

(a) 2 (b) 4 (c) 6 (d) 8 **[TIFR-2010]**

Soln. Using modular arithmetic ; $2^4 \equiv 6 \bmod 10$

Use property (iii) if $a \equiv b \pmod{n}$ then $a^P \equiv b^P \pmod{n}$

So we get $(2^4)^{20} = 6^{20} \pmod{10}$

$2^{80} = 6 \pmod{10}$

$\Rightarrow$ last digit of 2^{80} is 6

Hence, correct option is (c).

17. Which of the following statement is FALSE ?

(a) There exist a natural number which when divided by 3, leaves remainder 1 and which when divided by 4, leaves remainder 0.

(b) There exist a natural number which when divided by 6, leaves remainder 2 and which when divided by 9, leaves remainder 1.

(c) There exist a natural number which when divided by 7, leaves remainder 1 and which when divided by 11, leaves remainder 3.

(d) There exist a natural number which when divided by 12, leaves remainder 7 and which when divided by 8, leaves remainder 3. **[TIFR-2010]**

Soln. Apply modular arithmetic, check for option (b)

assume such natural number exist say x then $x \equiv 2 \bmod 6$ and $x \equiv 1 \bmod 9$

$\Rightarrow \quad x = 6q + 2$ and $x = 9q' + 1$

$\Rightarrow \quad 6q + 1 = 9q'$

$\Rightarrow \quad (6q+1) \bmod 9 = 0 \qquad \ldots (*)$

use $(a+b) \bmod n = (a \pmod{n} + b \pmod{n}) \bmod n$ then

$(6q+1) \bmod 9 = (6q \pmod 9) + 1 \pmod 9) \bmod 9$

$$\left.\begin{array}{ll} = & (0+1) \bmod 9 \\ \text{or} & (3+1) \bmod 9 \\ \text{or} & (6+1) \bmod 9 \end{array}\right\} \left.\begin{array}{r} = \;\; 1 \\ = \;\; 4 \\ = \;\; 7 \end{array}\right] \neq 0$$

which is contradiction to (*), hence option (b) is not true.

Hence, correct option is (b).

18. What is the last digit of 97^{2013} ?

(a) 1 (b) 3 (c) 7 (d) 9 **[TIFR-2014]**

Soln. By modular arithmetic

$$\begin{array}{lll} (97)^4 & \equiv 1 \bmod 10 & \\ ((97)^4)^{503} & \equiv 1 \bmod 10 & \text{by property (iii)} \\ 97^{2012} & \equiv 1 \bmod 10 & \\ 97^{2013} & \equiv 97 \bmod 10 & \text{by property (ii)} \\ & = 7 \bmod 10 & \end{array}$$

Hence, correct option is (c).

19. Which of the following primes satisfy the congruence $a^{24} \equiv (6a+2) \bmod 13$

(a) 41 (b) 47 (c) 67 (d) 83

Soln. $(41)^{24} \equiv (6.41+2) \bmod 13 \equiv (246+2) \bmod 13 \equiv (248) \bmod 13 \equiv 1 \bmod 13$

$(41^2)^{12} \equiv 1 \bmod 13$

Use Euler Theorem, $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$, $a = 41^2$; $n = 13$ then $a^{12} \equiv 1 \bmod 13$

Hence, correct options are (a) and (c).

20. The last two digit of 7^{81} are

(a) 07 (b) 17 (c) 37 (d) 47

Soln. $7^2 \equiv 49(\bmod 100)$

$\Rightarrow 7^4 \equiv 01(\bmod 100)$

$\Rightarrow (7^4)^{20} \equiv 1^{20}(\bmod 100)$

$\Rightarrow 7^{80} \equiv 1(\bmod 100)$

$\Rightarrow 7^{81} \equiv 07(\bmod 100)$

$\Rightarrow r = 07$

Hence, correct option is (a).

21. The last digit of $(38)^{2011}$ is

(a) 6 (b) 2 (c) 4 (d) 8

Soln. $38 \equiv 8 \ (\bmod 10)$

$(38)^4 \equiv (8)^4 \ (\bmod 10) = 6(\bmod 10)$

$((38)^4)^{502} \equiv 6 \ (\bmod 10)$

$(38)^{2008} \equiv 6 \ (\bmod 10)$

$\Rightarrow \quad (38)^{2009} \equiv 8 \ (\bmod 10)$

$\Rightarrow \quad (38)^{2010} \equiv 4 \ (\bmod 10)$

$\Rightarrow \quad (38)^{2011} \equiv \underset{\text{last digit}}{2} \ (\bmod 10)$

Hence, correct option is (b).

22. The unit digit of 2^{100} is

(a) 2 (b) 4 (c) 6 (d) 8

Soln. $2^4 \equiv 6 \ (\bmod 10)$

$(2^4)^{25} \equiv (6)^{25} \ (\bmod 10)$

$\Rightarrow 2^{100} \equiv 6 \ (\bmod 10)$

Hence, correct option is (c).

23. Let $m \le n$ be natural number. The number of injective maps from a set of cardinality m to a set of cardinality n is

(a) $m!$ (b) $n!$ (c) $\dfrac{n!}{(n-m)!}$ (d) None **[TIFR-2011]**

Soln. We know that number of one to one function is ${}^{n}P_m = \dfrac{n!}{(n-m)!}$

Hence, correct option is (c).

24. Number of surjective maps from a set of 4 elements to a set of 3 elements is

(a) 36 (b) 64 (c) 69 (d) 81

Soln. We know that number of onto function from a domain of *m* elements to a codomain of *n* elements is

$$n^m - \left[{}^nC_1(n-1)^m - {}^nC_2(n-2)^m + {}^nC_3(n-3)^m ..... \right]$$

here $m = 4$; $n = 3$

$$\Rightarrow \quad 3^4 - \left[{}^3C_1(3-1)^4 - {}^3C_2(3-2)^4 + {}^3C_3(3-3)^4 \right]$$

$$= 81 - \left[3(2)^4 - 3(1)^4 \right]$$

$$= 81 - [48 - 3] \Rightarrow 81 - 45 = 36$$

Hence, correct option is (a).

25. The number of element in the set $\{m : 1 \le m \le 1000,\ m \text{ and } 1000 \text{ are relatively prime}\}$ is

(a) 100 (b) 250 (c) 300 (d) 400

Soln. $\phi(1000) = \phi(10^3) = \phi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$

Hence, correct option is (d).

26. What is the cardinality of the set $\{z \in \mathbb{C} \mid z^{98} = 1 \text{ and } z^n \ne 1 \text{ for any } 0 < n < 98\}$?

(a) 0 (b) 12 (c) 42 (d) 49

Soln. Given group is isomorphic to cyclic group of order 98 i.e., $\mathbb{Z}_{98}$ then number of elements in $\mathbb{Z}_{98}$ which is coprime to 98 is $\phi(98) = 42$.

Hence, correct option is (c).

27. The number of positive divisor of 50,000 is

(a) 20 (b) 30 (c) 40 (d) 50

Soln. $n = 50,000 = 5 \times 10^4 = 2^4 \cdot 5^5$

$\tau(n) = (4+1)\,(5+1) = 5 \cdot 6 = 30$

Hence, correct option is (b).

28. The equation $x^{22} \equiv 2 \pmod{23}$ has

(a) no solution (b) 23 solution

(c) exactly one solution (d) 22 solution **[TIFR-2011]**

Soln. Use Euler theorem

$k = 22$; $a = 2$; $n = 23$; $d = \gcd(22, \phi(23)) = \gcd(22, 22) = 22$, then

$2^{\phi(23)/d} \equiv 1 \pmod{n} \Rightarrow 2^{22/22} \equiv 1 \pmod{23} \Rightarrow 2 \equiv 1 \pmod{23}$ which is a contradiction. Hence no solution exist.

Hence, correct option is (a)

29. If *n* is the positive integer such that the sum of all positive integer *a* satisfying $1 \le a \le n$ and $\gcd(a, n) = 1$ is equal to 240 *n* then number of summand namely $\phi(n)$ is

(a) 120 (b) 124 (c) 240 (d) 480

Soln. We know that

$$\sum_{\substack{(k,n)=1 \\ 1 \le k \le n}} k = \frac{1}{2} n \cdot \phi(n)$$

$$\Rightarrow \quad 240\,n = \frac{1}{2} n\, \phi(n) \quad \Rightarrow \quad \phi(n) = 480$$

Hence, correct option is (d)

30. Consider the equation $x^n \equiv 2\ (\text{mod}\,13)$. This equation has a solution for x if n equals

(a) 5 (b) 6 (c) 7 (d) 8

Soln. Use Euler theorem

$x^k \equiv a\ (\text{mod}\, n)$ has a solution iff $a^{\frac{\phi(n)}{d}} \equiv 1\,(\text{mod}\, n)$, where $d = \gcd(k, \phi(n))$

$\therefore\ \ x^n \equiv 2\ (\text{mod}\,13)$ has a solution iff $2^{12/d} \equiv 1\,(\text{mod}\ 13),\ \ d = \gcd(n, 12)$

If $n = 5$; $d = \gcd(5, 12) = 1 \;\Rightarrow\; 2^{12} \equiv 1\,(\text{mod}\ 13)$

$(2^6)^2 \equiv 1\,(\text{mod}\ 13)$

$(-1)^2 = 1\,(\text{mod}\ 13)$

$1 \equiv 1\,(\text{mod}\ 13) \to$ True

If $n = 6$; $d = \gcd(6, 12) = 6 \;\Rightarrow\; 2^{12/6} \equiv 1\,(\text{mod}\ 13)$

$\Rightarrow\ \ 2^2 \equiv 1\,(\text{mod}\ 13) \quad \Rightarrow \quad 4 \equiv 1\,(\text{mod}\ 13) \to$ Not true

If $n = 7 \;\Rightarrow\; d = \gcd(7, 12) = 1 \to$ True as $(n = 5)$

If $n = 8 \;\Rightarrow\; d = \gcd(8, 12) = 4$

$\Rightarrow\ \ 2^{12/4} \equiv 1\,(\text{mod}\ 13) \quad \Rightarrow \quad 2^3 \equiv 1\,(\text{mod}\ 13) \quad \Rightarrow \quad 8 \equiv 1\,(\text{mod}\ 13) \to$ Not true

Hence, correct options are (a) and (c)

31. The last two digits of the number $9^{(9^9)}$ is

(a) 29 (b) 89 (c) 49 (d) 69 **[D.U. 2016]**

Soln. $9^k = (10-1)^k = 10^k + kc_1 10^{k-1} + \ldots .10 \cdot k - 1$

$9^k \bmod 100 \equiv (10 \cdot k - 1) \bmod 100$

$10 \cdot k \equiv 10 \cdot i\,(\text{mod}\,100)$ where i is last digit of k.

so $10 \cdot k - 1 \equiv 10 \cdot i - 1(\text{mod}\,100)$

$\Rightarrow\ 9^9 \equiv 89\,(\text{mod}\,100)$ as $k = 9$ and $i = 9$.

$\Rightarrow\ 9^{9^9} = 89\,(\text{mod}\ 100)$ as $k = 9^9,\ i = 9$

Hence, correct option is (b).

32. The total number of subsets of a set of 6 element is

(a) 720 (b) 6^6 (c) 21 (d) None **[TIFR-2010]**

Soln. By definition

Total number of subsets of a set of cardinality n is 2^n, so here $n = 6 \;\Rightarrow\; 2^6$

Hence, correct option is (d).

33. True or False

There exist a set $A \subset \{1, 2, \ldots, 100\}$ with 65 element such that 65 cannot be expressed as a sum of two element of A

Ans. True **[TIFR-2011]**

Soln. Take $A = \{36, 37, \ldots., 100\}$, then sum of any two elements of A exceeds 65.

34. Which of the following statement (s) is/are correct ?

(a) $\left|\underline{166}\right. \equiv 1\left(\text{mod}\,167\right)$ (b) $\left|\underline{181}\right. \equiv 1\left(\text{mod}\,181\right)$

(c) $\left|\underline{166}\right. + 2 \equiv 1\left(\text{mod}\,167\right)$ (d) $\left|\underline{180}\right. \equiv 180\left(\text{mod}\,181\right)$

Soln. By wilson's theorem

$\underline{|p-1} \equiv -1 \pmod{p}$ p is prime ...(i)

Also $-1 \equiv p-1 \pmod{p}$ ...(ii)

adding (i) and (ii)

$\underline{|p-1} \equiv p-1 \pmod{p}$

for $p = 181$,

$\underline{|180} \equiv 180 \pmod{181}$

$\therefore$ option (d) is correct

Option (c) can be written has

$\underline{|166} \equiv -1 \pmod{167}$, by wilson's theorem

option (c) is correct

and (b) (d) are false

Correct option are (a) and (c)

35. Let m,n are distinct primes, then $m^{n-1} + n^{m-1} - 1$ is

(a) multiple of $m + n$ (b) multiple of mn (c) multiple of mn^2 (d) multiple of m^2n^2

Soln. $m \mid m^{n-1}$ ....(i)

$n^{m-1} \equiv 1 \pmod{m}$

from (i)

i.e., $m \mid n^{m-1} - 1$

$m \mid n^{m-1} + m^{n-1} - 1$

similarly, $n \mid n^{m-1} + m^{n-1} - 1$

$\therefore$ $n^{m-1} + m^{n-1} - 1$ is a multiple of mn

$\therefore$ (b) is correct

Take m = 2, n = 3

Then $m^{n-1} + n^{m-1} - 1 = 2^2 + 3^1 - 1 = 6$ is not divisible by mn^2

= 18 and $m + n$ = 5.

$\therefore$ (c), (d), (a) false

Option (b) is correct

36. Which of the following statement is true ?

(a) The sum of all positive integers less than 17 and prime to 17 is 126

(b) $n^5 - n$ is divisible by 30.

(c) $n^5 - n$ is not divisble by 30.

(d) None of these

Soln. The sum of all positive ingers which are less than n and prime to n is $\frac{1}{2} n\,\phi(n)$

$\therefore$ sum of positive integers which are less then 17 and prime to 17 is $= \frac{1}{2} 17 \times 16 = 136$

Option (a) is not true

Since 5 is prime, therefore by fermat’s theorem, we have

$n^5 \equiv n(\text{mod } 5)$

i.e. $5 | n^5 - n$

Also $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1)$ ...(i)

$= (n-1)n(n+1)(n^2+1)$

Now, $(n-1)n(n+1)$ is a product of thre consecutive integers and soit is divisible $\underline{|3} = 6$

then $6 | n^5 - 5$ ...(ii)

Since $(5, 6) = 1$ i.e. 5 and 6 are relatively prime therefore from (i) and (ii)

we have $(5 \cdot 6) | n^5 - n$

$\Rightarrow 30 | n^5 - n$

$\therefore$ option (b) is correct and option(c) is false

Correct option is (b)

37. Which of the following is/are not true ?

(a) Union of two equivalence relation on a set is necessarily an equivalence relation.

(b) The intersection of two equivalence relation on a set is an equivalence relation on the set.

(c) Every number of the form $2^p - 1$ is a prime, where p is prime.

(d) None of these

Soln. Let $A = \{a, b, c\}$ and let R, S be two relation on A given by.

$R = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$

$S = \{(a,a),(b,b),(c,c),(b,c),(c,b)\}$

Here R and S are equivalence relation on A

But $R \cup S$ is not transitive because $(a,b) \in R \bigcup S$ and $(b,c) \in R \bigcup S$ but $(a,c) \notin R \bigcup S$

Hence RUS is not an equivalcne relation on A

$\therefore$ option (a) is not nessarily true

So (a) is correct

Otpion (b) is true

$\therefore$ option (b) is false

The numbers of the form $2^n - 1$, where n is a prime are known as Mersenne number

All Mersenne numbers are not prime

2047 = 2^{11}–1 = 2047 is

Composite mersenne number.

option (c) is not necessarily true

$\therefore$ option (c) is correct

$\therefore$ option (a), (c) are correct

PRACTICE SET–1

[Single Correct Answer Type Questions]

1. The collection of intelligent students in a class is

(*a*) Null set (*b*) A single ton set
(*c*) A finite set (*d*) Not a well defined collection

2. If the set *A* has *p* elements, *B* has *q* elements, then the number of elements in $A \times B$ is

(*a*) $p+q$ (*b*) $p+q+1$ (*c*) pq (*d*) p^2

3. If *A* and *B* are two sets, then $A \times B = B \times A$ if and only if

(*a*) $A \subseteq B$ (*b*) $B \subseteq A$ (*c*) $A = B$ (*d*) None of these

4. The relation "less than" in the set of natural numbers is

(*a*) Only symmetric (*b*) Only transitive
(*c*) Only reflexive (*d*) Equivalence relation

5. For real numbers *x* and *y*, we write $x\ R\ y \Leftrightarrow x - y + \sqrt{2}$ is an irrational number. Then the relation *R* is

(*a*) Reflexive (*b*) Symmetric (*c*) Transitive (*d*) None of these

6. Let *R* be a reflexive relation on a finite set *A* having *n*-elements and let there be *m* ordered pairs in *R*. Then

(*a*) $m \ge n$ (*b*) $m \le n$ (*c*) $m = n$ (*d*) None of these

7. Let *R* be a reflexive relation on a set *A* and *I* be the identity relation on *A*. Then

(*a*) $R \subset I$ (*b*) $I \subseteq R$ (*c*) $R = I$ (*d*) None of these

8. The relation "is subset of" on the power set $P(A)$ of a set *A* is

(*a*) Symmetric (*b*) Anti-symmetric
(*c*) Equivalence relation (*d*) None of these

9. If *n* and *m* are positive integer and $n^9 = 19m + r$, then the possible value for *r* modulo 19 are

(a) only 0 (b) only $0, \pm 1$ (c) only ± 1 (d) none of these **[TIFR-2010]**

[Multiple Correct Type Questions]

1. Define a relation ρ on the set of positive integers $\mathbb{Z}^+$ by $x\ \rho\ y$ if and only if g.c.d. of *x* and *y* is bigger than 1. Then the relation ρ is

(*a*) Reflexive and symmetric but not transitive
(*b*) Symmetric and transitive but not reflexive
(*c*) Symmetric but neither reflexive nor transitive
(*d*) An equivalence relation

2. Which of the following is an equivalence relation in $\mathbb{R}$:

(*a*) $x \le y$ for all $x, y \in \mathbb{R}$ (*b*) $x - y$ is an irrational number
(*c*) $x - y$ is divisible by 3 (*d*) $x - y$ is a perfect square

3. Which of the following is/are correct

(*a*) Two equivalence classes are either identical or disjoint
(*b*) The quotient set of a set *S* relative to an equivalence relation on *S* is a subset of *S*.
(*c*) Equivalence class of an equivalence relation on *S* is a subset of *S*.
(*d*) A partition of a set *S* into subsets defines an equivalence relation on *S*.

4. Let A be set of all polynomials with real coefficients. For $f, g \in A$ and $f\ R\,g$ if $f' = g'$ where $f' =$ derivative of f, g' = derivative of g. Then choose the incorrect answer

(*a*) For any $f \in A$, class of $f = \{f + c : c \text{ is real}\}$ (*b*) R is an anti-symmetric relation

(*c*) R is an equivalence relation (*d*) None of these

5. A non-trivial binary relation R on a non-empty set X is called

(*a*) Symmetric if $x\ R\ y \Leftrightarrow y\ R\ x$

(*b*) Anti-symmetric if $x\ R\ y$ and $y\ R\ x \Rightarrow x = y$

(*c*) Reflexive if $x\ R\ x$ holds for all x in X

(*d*) Transitive if $x\ R\ y$ and $y\ R\ z \Rightarrow x\ R\ x$

[Numerical Answer Type Questions]

1. If $Q = \left\{ x : x = \dfrac{1}{y}, \text{ where } y \in \mathbb{N} \right\}$, and if $Q \subset \mathbb{N}$, then $|Q| = ??$

2. Gives two finite sets A and B such that $n(A) = 2, n(B) = 3$. Then total number of relations from A to B is_______??

3. The number of elements in the set $\{m : 1 \le m \le 1000, m \text{ and } 1000 \text{ are relatively prime}\}$ is_______??

4. The unit digit of 2^{100} is_______??

5. The number of reflexive relations on a set of cardinality 3 is_______??

6. A relation R is defined from {2, 3, 4, 5} to {3, 6, 7, 10} by $x\ R\ y \Leftrightarrow x$ is relatively prime to y. Then cardinality of domain of R is_______??

7. True or False

If n is not a multiple of 23 then the remainder when n^{11} divided by 23 is ± 1.

PRACTICE SET (1) SOLUTIONS

[Single Correct Answer Type Questions]

1. (*d*), since there is no definite definitions of intelligence, (word intelligence is not well defined).

2. (*c*) $p\ q$

3. (*d*) None of these, since $A = \{\ \}$ and B = any non empty set then in both cases $A \times B = B \times A$, but $A \ne B$.

4. (*b*) only transitive

5. (*a*) Reflexive

not symmetric. since $x = \sqrt{2}, y = 1$ then $x\ R\ y$, since $\sqrt{2} - 1 + \sqrt{2} = 2\sqrt{2} - 1 \in \mathbb{Q}^C$ but $y \cancel{R} x$, since $1 - \sqrt{2} + \sqrt{2} = 1 \notin \mathbb{Q}$. Similarly we can show for transitive.

6. (*a*) $m \ge n$. since if it has *n*-elements and relation is reflexive then it contains the identity relation and so contains atleast *n* ordered pairs.

7. $(b) \cdot I \subseteq R$

8. (*b*) Anti-symmetric. since if $A\ R\ B$ then $A \subseteq B$. And also if $B\ R\ A \Rightarrow B \subseteq A \Rightarrow \boxed{A = B}$

9. (*c*)

[Multiple Correct Type Questions]

1. (*c*) symmetric but neither reflexive nor transitive.

Not reflexive since 1 does not belong under this relation.

Not transitive since (2, 10) = 2 and (10, 15) = 5 but (2, 15) = 1 which is not bigger than 1. so, $2\ \rho\ 10$ and $10\ \rho\ 15$ but $2 \not\rho\ 15 \Rightarrow$ not transitive

2. (*c*) $(x-y)$ is divisible by 3.

3. (*a*), (*b*), (*c*), (*d*).

(*b*) Since quotient set contains all disjoint classes of a set *S* of an equivalence relation. Hence, it is a subset of *S*.

(*d*) Since to each partition of a set *S* defines an equivalence relation on *S*.

4. (*a*), (*c*)

5. (*a*), (*b*), (*c*)

[Numerical Answer Type Questions]

1. $|Q|=1$, since only for $1\in N$ s.t. $x=\frac{1}{1}=1\in Q\subseteq \mathbb{N}$.

2. 64. Total number of relations from A to $B=2^{n(A)\times n(B)}=2^{2\cdot 3}=2^6=64$.

3. $\phi(1000)=\phi(2^3\cdot 5^3)=\phi(2^3)\cdot\phi(5^3)=(2^3-2^2)\cdot(5^3-5^2)=(4)\,(100)=400$

4. $2^1=2$

$2^2=4$

$2^3=8$

$2^4=16$

$2^5=32$

so $(2^{100})=(2^{5\times 20})=(2^5)^{20}=(2)^{20}=2^5\cdot 2^5\cdot 2^5\cdot 2^5=2\cdot 2\cdot 2\cdot 2=16=6$

so, Ans. 6. since we get 2 on unit place if we take 5 power of 2. So we reduce 100 into 5 × 20, then again reduce 2^{20} into $2^5\cdot 2^5\cdot 2^5\cdot 2^5$ and then find the value at unit place.

5. Since number of reflexive relation $=2^{n^2-n}=2^{9-3}=2^6=64$

6. (2, 3), (2, 7), (3, 7), (3, 10), (4, 3), (4, 7), (5, 3), (5, 7)

so domain is {2, 3, 4, 5}. Hence cardinality of domain of *R* = 4.

7. True

Chapter 2

GROUP, ABELIAN, ORDER OF ELEMENTS, SUBGROUPS

1. **Binary operation:** Let G be a non empty set. A binary operation on G is a function from $G \times G$ to G i.e. binary operation on G assigns each ordered pair of elements of G to exactly one element of G.

Examples: Ordinary addition, subtraction, multiplication of integers.

Division of integers is not a binary operation.

Example :

(i) $(\mathbb{N}, -)$ is not binary operation as $3 \in \mathbb{N}, 4 \in \mathbb{N}$ but $3 - 4 = -1 \notin \mathbb{N}$

(ii) $(\mathbb{Q}^c, \times)$ set of all irrational numbers with the operation multiplication. As $\sqrt{2} \in \mathbb{Q}^c$ but $\sqrt{2} \times \sqrt{2} = 2 \notin \mathbb{Q}^c$

Thus '×' multiplication not a binary operation on $\mathbb{Q}^c$.

(iii) 'U' union of sets is binary on the set of all subsets of set of natural numbers.

2. **Group:** Let G be a non-empty set together with a binary operation$*$ (usually called multiplication). We say G is a group under this operation if the following three properties are satisfied.

(i) Associativity: The binary operation is associative, i.e. $(a*b)*c = a*(b*c), \forall a, b, c \in G$.

(ii) Existence of Identity: There is an element e (called the identity) in G, such that $a*e = e*a = a$ for all a in G.

(iii) Existence of inverse : For each element 'a' in G there is an element 'b' called inverse of 'a' in G such that $a*b = b*a = e$.

Example :

(i) $(\mathbb{N}, -)$ is not a group since (–) fails to be a binary operation.

(ii) $(\mathbb{N}, +)$ is not a group. It is binary and associative but fails to have an identity element.

(iii) $(\mathbb{Q}^c \cup \{0\}, +)$ is not binary, since $\left(-\sqrt{2}\right) \in \mathbb{Q}^c$ also $\left(1+\sqrt{2}\right) \in \mathbb{Q}^c$ but $\left(1+\sqrt{2}\right) + \left(-\sqrt{2}\right) = 1 \notin \mathbb{Q}^c$
Hence not a binary. So not a group

3. **Abelian Group:** A group G is called abelian group if for each $a, b \in G$, we have $ab = ba$.

Example :

(i) Every group of prime order is always abelian.

(ii) Upto order 5, all groups always abelian.

(iii) Group G of all $n \times n$, non-singular matrices with operation ordinary matrix multiplication with real entries is not abelian. Let $n = 2$.

Let $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, B = \begin{bmatrix} 1 & 4 \\ 3 & 1 \end{bmatrix} \in G$

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 6 \\ 9 & 3 \end{bmatrix}$$

$$BA=\begin{bmatrix}1 & 4\\ 3 & 1\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}=\begin{bmatrix}1 & 14\\ 3 & 9\end{bmatrix}$$

Clearly $AB \neq BA$. Hence, G is not abelian

Note: But operation is matrix addition with $n \times n$ matrices, then it is abelian group.

4. Examples: Groups

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ under ordinary addition are groups with identity zero and inverse of a is – a.

(ii) Set of all 2 × 2 matrices with real entries is a group under componentwise addition.

(iii) The set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in $\mathbb{Z}_n$ the inverse of j is $-j$. This group is usually referred to as the group of integers modulo n.

(iv) The set $\mathbb{R}^*$ of non-zero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $1/a$.

(v) The set $GL(2,\mathbb{R}) = \left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} : a,b,c,d \in \mathbb{R}, ad \neq bc\right\}$ of 2 × 2 matrices with real entries and non-zero determinant is a non abelian group under the operation matrix multiplication, $GL(2,\mathbb{R})$ is called general linear group of 2 × 2 matrices over $\mathbb{R}$.

5. Elementary Properties of Groups:

1. Uniqueness of the identity: The identity element in a group is unique.

Proof: Suppose e and e' are two identity element of a group G. Then

$ee' = e$ if e' is identity and $ee' = e'$ if e is identity.

$\Rightarrow e = e'$

Hence identity element is unique.

2. Uniqueness of inverse: The inverse of each element of a group is unique.

Proof: Let 'a' be any element of a group G and let 'e' be the identity element. Suppose b and c are two inverses of a i.e.

$ba = e = ab$ and $ca = e = ac$

We have $b(ac) = be$ $[\because ac = e]$

$= b$ $[\because e$ is identity$]$

Also $(ba)c = ec$ $[\because ba = e]$

$= c$ $[\because e$ is identity$]$. Thus we get $b = c$

3. If the inverse of a is a^{-1}, then the inverse of a^{-1} is a i.e. $(a^{-1})^{-1} = a$.

4. Theorem: (Reversal rule)To prove that $(ab)^{-1} = b^{-1}a^{-1}, \forall a, b \in G$. i.e. the inverse of the product of two elements of a group G is the product of the inverses taken in the reverse order.

Proof: Suppose a and b are elements of G. If a^{-1} and b^{-1} are inverses of a and b respectively.

Then $a^{-1}a = e = aa^{-1}$ where e is the identity element.

and $b^{-1}b = e = bb^{-1}$

Now, $(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$

$= [a(bb^{-1})]a^{-1}$ [by associatively]

$= [ae]a^{-1} [\because bb^{-1} = e]$

$= aa^{-1} [\because ae = a]$

$= e \; [\because aa^{-1} = e]$

Also $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)] \; = \; b^{-1}[(a^{-1}a)b] = b^{-1}(eb) = b^{-1}b = e$

Thus we have $(b^{-1}a^{-1})(ab) = e = (ab)(b^{-1}a^{-1})$

$\therefore$ By definition of inverse, we have $(ab)^{-1} = b^{-1}\; a^{-1}$

> If the group is commutative, then we shall have $(ab)^{-1} = a^{-1}b^{-1}$
> Since $b^{-1}a^{-1} = a^{-1}b^{-1}$

5. **Theorem:** Cancellation laws: If *G* is a group with binary operation, then the left and right cancellation laws hold in *G*, that is $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ for all $a, b, c \in G$.

Proof: Suppose, *ab* = *ac*,

Since $a \in G \Rightarrow a^{-1} \in G$

Premultiplying both sides by a^{-1}, we have $a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [by associatively]

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Similarly, from $ba = ca$, one can deduce that $b = c$ upon multiplication on the right by a^{-1}.

6. **Theorem:** If *G* is a group with binary operation and if *a* and *b* be any elements of *G*, then the linear equation $ax = b$ and $ya = b$ have unique solutions in *G*.

7. **Semi-Group:** A semi group is a set with an associative binary operation.

Example :

(*i*) $\mathbb{N}$ – set of natural number under addition is a semi-group.

$* - l.c.m. \, (a, b)$ where $a, b \in \mathbb{N}$. So, '*' is binary operation Also '*' is associative. Hence ($\mathbb{N}$, *) is a semi-group.

(*ii*) $(\mathbb{Z}, -)$ set of all integers with the operation subtraction is not a semigroup since it does not hold associativity.

Let $12, 1, 10 \in \mathbb{Z}$.

As, $(12 - 1) - 10 = 11 - 10 = 1$

$12 - (1 - 10) = 12 - (-9) = 12 + 9 = 21$

So, $(12 - 1) - 10 \neq 12 - (1 - 10)$

8. **Cancellation laws may not hold in a semi-group:**

(i) Consider the set of all 2 × 2 matrices over integers under matrix multiplication which forms a semi-group

If we have $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$

Then $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, But $B \neq C$

(ii) Set of natural numbers under addition is an example of a semi-group in which cancellation laws hold.

Theorem : A finite semi-group in which cancellation laws hold is a group.

Remark: The above theorem holds only in finite groups. The semi-group of natural numbers under addition being an example where cancellation laws hold but this is not a group.

1. **Order of a Group:** The number of elements of a group (finite or infinite) is called its order. We will use $o(G)$ or $|G|$ to denote the order of G.

Exp: The group $\mathbb{Z}$ of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 has order 4.

2. **Sub-group:** If a subset H of a group G is itself a group under the operation of G, we say H is a subgroup of G.

We use the notation $H \leq G$ to mean H is a subgroup of G. If H is a sub-group of G but not equal to G then we write $H < G$, i.e. proper subgroup of G.

$\mathbb{Z}_n$ under addition modulo n is not a subgroup of $\mathbb{Z}$, because binary operations are different.

If G is a group, then G and $\{e\}$ are improper subgroup of G. All other subgroups are proper subgroups.

Examples: (i) $2\mathbb{Z}$ i.e. set of even integers under addition is a subgroup of $\mathbb{Z}$.

(ii) $\mathbb{Q}^+$ under multiplication is a proper subgroup of $\mathbb{R}^+$ under multiplication.

3. **Prob.** Show that if H is any subgroup of G, then $H^{-1} = H$. Also show that the converse is not true.

Soln. **Part-1:** $H^{-1} = \{h^{-1} \mid h \in H\}$

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

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

Now $h \in H \Rightarrow h^{-1} \in H$ ($\because H$ is sub-group)

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

Let $a \in H$

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

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

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

$\Rightarrow H \subseteq H^{-1}$

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

Part-2: If H is a subset of a group G and $H^{-1} = H$, then it is not necessary that H is a subgroup of G, for example $H = \{-1\}$ is a subset of the multiplicative group $G = \{1,-1\}$. Also $H^{-1} = \{-1\}$ as -1 is the inverse of -1 in G. But $H = \{-1\}$ is not a subgroup of G. We have $(-1)(-1) = 1 \notin H$. Thus H is not closed with respect to multiplication.

4. **(a):** Show that if H is any subgroup of a group G. Then $HH = H$

Soln.: Let h_1h_2 be any element of HH where $h_1 \in H, h_2 \in H$. Since H is a subgroup of G, therefore

$h_1h_2 \in H \Rightarrow h_1h_2 \in H$

$\therefore HH \subseteq H$

Now let h be any element of H.

Then we can write $h = he$ where e is the identity element of G. Now $he \in HH$, since $h \in H, e \in H$

Thus, $H \subseteq HH$,

Hence $HH = H$

5. **(b):** Let *H*, *K* be subgroups of *G*. Show that *HK* is a subgroup of *G* iff $HK = KH$.

Proof : Let *HK* be a subgroup of *G*. We show *HK* = *KH*.

Let $x \in HK$ be any element

Then $x^{-1} \in HK$ (as *HK* is a subgroup)

$\Rightarrow x^{-1} = hk$ for some $h \in H, k \in K$

$\Rightarrow x = (hk)^{-1} = k^{-1}h^{-1} \in KH$

thus, $HK \subseteq KH$

Again let $y \in KH$ be any element

Then $y = kh$ for some $k \in K, h \in H$

$\Rightarrow y^{-1} = h^{-1}k^{-1} \in HK \Rightarrow (y^{-1})^{-1} \in HK$ (as *HK* is a subgroup)

$\Rightarrow y \in HK$

$\Rightarrow KH \subseteq HK$

Hence, *HK* = *KH*

Conversely, let *HK* = *KH*.

Let $a, b \in HK$ be any two elements, we show $ab^{-1} \in HK$

Let $a, b \in HK \Rightarrow a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$

Then $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}$

Now, $(k_1k_2^{-1})h_2^{-1} \in KH = HK$

thus $(k_1k_2^{-1})h_2^{-1} = hk$ for some $h \in H, k \in K$

Then $ab^{-1} = h_1(hk) = (h_1h)k \in HK$

Hence, *HK* is subgroup.

Criterion for a complex to be a Subgroup.

6. **Theorem:** (Two step subgroup test): A non-empty subset *H* of a group *G* is a subgroup of *G* if and only if

(i) $a \in H, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of *a* in *G*.

Proof : Let *H* be a subgroup of *G* then by definition it follows that (i) and (ii) hold.

Conversely, let the given conditions hold in *H*.

Closure: From (i), we have $a \in H, b \in H \Rightarrow ab \in H$

Associativity: $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a(bc) = (ab)c$

Identity: For any $a \in H$, $a^{-1} \in H$ [by (ii)]

So, $a \in H$, $a^{-1} \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$

Inverse: Inverse of each element of *H* is in *H* by (ii). Thus *H* is a group and therefore a subgroup of the group *G*.

7. Theorem: (one step subgroup test): A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof : If H is a subgroup of G then,

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

$\Rightarrow ab^{-1} \in H$ [closure prop. of H]

Conversely, let the given condition hold in H. i.e. $a, b \in H \Rightarrow ab^{-1} \in H$.

Associativity: $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow (ab)c = a(bc)$

Identity: Let $a \in H$ be any element of H (as H is non-empty), then $a \cdot a^{-1} \in H$ (after taking $b = a$)

$\Rightarrow e \in H$

So, H has identity.

Inverse: Again, for any $a \in H$ and as $e \in H$, $ea^{-1} \in H \Rightarrow a^{-1} \in H$

i.e. H has inverse of each element

Closure: Finally, for any $a, b \in H$

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

i.e. H is closed under multiplication

Hence, H forms a group and therefore a subgroup of G.

8. **Theorem:** A non-empty finite subset H of a group G is a subgroup of G iff H is closed under multiplication (binary operation).

Proof: If H is a subgroup of G then it is closed under multiplication by definition of group.

Conversely, let H be a finite subset such that $a, b \in H \Rightarrow ab \in H$

Associativity: Now, $a, b, c \in H \Rightarrow a, b, c \in G$

[Associativity in G] $a(bc) = (ab)c$

$\Rightarrow$ Associativity holds in H.

This implies H is a semi-group.

Again, the cancellation laws hold in H, as they hold in G, and thus H is a finite semi-group in which cancellation laws hold. Hence H forms a group.

Remarks : If H is infinite then H may not be a subgroup

Example : $H = \mathbb{N} \subset \mathbb{R}$, then H is closed under addition but not a group.

9. **Corollary (i):** A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup that $HH^{-1} \subseteq H$.

Proof: The condition is necessary: It is given that H is a subgroup of G,

Let ab^{-1} be any arbitrary element of HH^{-1}, where $a \in H, b \in H$.

Since H itself is a group, therefore, $b \in H \Rightarrow b^{-1} \in H$

Thus, $a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$ [by closure property]

$ab^{-1} \in HH^{-1} \Rightarrow ab^{-1} \in H$

Hence, $HH^{-1} \subseteq H$

The condition is sufficient: It is given that $HH^{-1} \subseteq H$.

Let $a, b \in H$. Then $ab^{-1} \in HH^{-1}$.

Since $HH^{-1} \subseteq H$

therefore $ab^{-1} \in HH^{-1} \Rightarrow ab^{-1} \in H$.

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

Hence, *H* is a subgroup of *G*.

Corollary (ii): A necessary and sufficient condition for a non-empty subset *H* of a group *G* to be a subgroup is that $HH^{-1} = H$.

Proof : The condition is necessary: Suppose *H* is a subgroup of *G*. Then by corollary (i), $HH^{-1} \subseteq H$.

Now, *H* is a subgroup of *G*, therefore $e \in H$. If *h* is any arbitrary element of *H*, then

$h = he = he^{-1} \in HH^{-1} [\because h \in H, e^{-1} \in H^{-1}]$

$\therefore H \subseteq HH^{-1}$

Hence, $HH^{-1} = H$

The condition is sufficient: It is given that $HH^{-1} = H \ \therefore HH^{-1} \subseteq H$

Hence, by corollary (i), *H* is subgroup of *G*.

Criterion for the product of two subgroups to be a subgroup.

10. **Theorem:** If *H*, *K* are two subgroups of a group *G*, then *HK* is a subgroup of *G* iff *HK* = *KH*

Proof: Let *H* and *K* be any two subgroups of a group *G*. Let *HK* = *KH* [In order to prove that *HK* is subgroup of *G* it is sufficient to prove that $(HK)(HK)^{-1} = HK$]

We have, $(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1}) = H(KK^{-1})H^{-1} = (HK)H^{-1}$ [$\because$ *K* is a subgroup $\Rightarrow KK^{-1} = K$] $= (KH)H^{-1}$ [$\because$ $HK = KH$] $= K(HH^{-1}) = KH$ [$\because$ *H* is a subgroup $\Rightarrow HH^{-1} = H$] = *HK*.

$\Rightarrow HK$ is a subgroup of *G*.

Conversely, suppose that *HK* is a subgroup.

Then, $(HK)^{-1} = HK \Rightarrow K^{-1}H^{-1} = HK$

$\Rightarrow KH = HK$ [$\because$ *K* is a subgroup $\Rightarrow K^{-1} = K$ and similarly $H^{-1} = H$]

Corollary: If *H*, *K* are two subgroups of an abelian group *G*, then *HK* is a subgroup of *G*.

Proof: We know that if *H*, *K* are two subgroups of a group *G* then *HK* is a subgroup of *G* iff $HK = KH$. Since the given group *G* is abelian, therefore we have *HK* = *KH*. Hence *HK* is a subgroups of *G*.

11. **Theorem:** If H_1 and H_2 are two subgroups of a group *G*, then $H_1 \cap H_2$ is also a subgroup of *G*.

Proof: Let H_1 and H_2 be any two subgroups of *G*. Then $H_1 \cap H_2 \neq \phi$, since atleast the identity element '*e*' is common to both H_1 and H_2.

In order to prove that $H_1 \cap H_2$ is a subgroup, it is sufficient to prove that, if $a \in H_1 \cap H_2$,

$b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Let $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$ and $b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1 and H_2 are subgroups,

therefore, $a \in H_1, b \in H_1 \Rightarrow ab^{-1} \in H_1$ and $a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally, $ab^{-1} \in H_1, ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \bigcap H_2$

thus we have shown that

$a \in H_1 \bigcap H_2, b \in H_2 \bigcap H_2 \Rightarrow ab^{-1} \in H_1 \bigcap H_2$

Hence $H_1 \bigcap H_2$ is a subgroup of G.

13. **Theorem:** Arbitrary intersection of sub-groups of a group is a subgroup.

$H_1 \bigcap H_2$ is the largest subset of G which is contained in H_1 as well as in H_2.
Therefore, $H_1 \bigcap H_2$ is the largest subgroup of G contained in H_1 and H_2

14. The union of two subgroups is not necessarily a subgroup. e.g. Let G be the additive group of integers. Then H_1 = {...., –6, –4, –2, 0, 2, 4, 6, ...}
and H_2 = {...., –12, –9, –6, –3, 0, 3, 6, 9, 12, ...} are both subgroups of G.

We have $H_1 \bigcup H_2$ = {..., –4, –3, –2, 0, 2, 3, 4, 6, ...} Obviously $H_1 \bigcup H_2$ is not closed with respect to addition as $2 \in H_1 \bigcup H_2, 3 \in H_1 \bigcup H_2$ but $2 + 3 = 5 \notin H_1 \bigcup H_2$. Therefore, $H_1 \bigcup H_2$ is not a subgroup of G.

15. **Problem:** Show that the union of two subgroups is a subgroup if and only if one is contained in the other.

Soln: Suppose H_1 and H_2 are two subgroups of a group G. Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Then $H_1 \bigcup H_2 = H_2$ or H_1. But H_1 and H_2 are subgroups and therefore, $H_1 \bigcup H_2$ is also subgroup.

Conversely, suppose $H_1 \bigcup H_2$ is a subgroup. To prove that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Let us assume that H_1 is not a subset of H_2 and H_2 is also not a subset of H_1.
Now, H_1 is not a subset of H_2

$\Rightarrow \exists a \in H_1$ and $a \notin H_2$ ... (i)

and H_2 is not a subset of H_1

$\Rightarrow \exists b \in H_2$ and $b \notin H_1$ ... (ii)

From (i) and (ii), we have, $a \in H_1 \bigcup H_2$ and $b \in H_1 \bigcup H_2$

Since $H_1 \bigcup H_2$ is a subgroup, therefore $ab = c$ (say) is also an element of $H_1 \bigcup H_2$.

$\Rightarrow$ either $ab \in H_1$ or $ab \in H_2$

If $ab = c \in H_1$ then $b = a^{-1}c \in H_1$ [$\because H_1$ is a subgroup, therefore $a \in H_1 \Rightarrow a^{-1} \in H_1$]

But from (ii), we have, $b \notin H_1$. Thus we get a contradiction.

Again, suppose $ab = c \in H_2$

Then $a = cb^{-1} \in H_2$ [$\because$ H_2 is a subgroup, therefore $b \in H_2 \Rightarrow b^{-1} \in H_2$]

But, from (i), we have $a \notin H_2$. Thus here also we get a contradiction.

Hence, either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

16. **Centre of a group:** The centre Z(G), of a group G is the subset of elements in G that commute with every element of G. In symbols

$Z(G) = \{a \in G : ax = xa \text{ for all } x \text{ in } G\}$

Example :--

(*i*) Find the centre of Q_8, where Q_8 is Quaternion group.

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

$Z(Q_8) = \{+1, -1\}$, no other element belongs to the centre of Q_8. Since $i \cdot j = k$ but $j \cdot i = -k$ and $k \neq -k$. Similarly, we can show that $k \notin Z(Q_8)$. Only $\{-1, +1\}$ are the elements which commutes with all the elements of Q_8.

(*ii*) Find the centre of K_4.

We have, that K_4 is abelian. So each element commutes with all the elements and so, $Z(G) = K_4$.

So, for any group *G* which is abelian, $\boxed{Z(G) = G}$.

17. **Theorem:** The centre of a group *G* is a subgroup of *G*.

Proof: The identity '*e*' of a group *G* commutes with every element of *G*, therefore *Z*(*G*) is non-empty. Now, suppose $a, b \in Z(G)$.

Then $ax = xa$ and $bx = xb$ for all $x \in G$

$\Rightarrow a^{-1}axa^{-1} = a^{-1}xaa^{-1} \Rightarrow xa^{-1} = a^{-1}x$

and $b^{-1}bxb^{-1} = b^{-1}xbb^{-1} \Rightarrow xb^{-1} = b^{-1}x$

Now, $x(ab^{-1}) = (xa)b^{-1} = (ax)b^{-1} = a(xb^{-1}) = (ab^{-1})x$ for all $x \in G$.

Thus, $a, b \in Z(G) \Rightarrow ab^{-1} \in Z(G)$. Hence, $Z(G)$ is a subgroup of *G*.

18. **Centralizer (Normalizer) of '*a*' in *G*:** Let '*a*' be a fixed element of a group *G*. The centralizer of *a* in *G*, *C*(*a*) or *N*(*a*), is the set of all elements in *G* that commute with '*a*'. In symbols

$C(a) = \{g \in G : ga = ag\}$

Example :

(*i*) Find *N*(*i*) in Q_8?

$N(i) = \{1, -1, i, -i\}$

Since 1 and –1 already in $Z(Q_8)$. So they will commute with *i*. Also $i \cdot i = -1 = i \cdot i \Rightarrow i \in N(i)$. Infact, each element commute with itself for any group.

again, $i\,(-i) = -(-1) = 1 = (-i)\,i \Rightarrow -i \in N(i)$

but $j \notin N(i)$ since $\boxed{i\,j \neq j\,i}$.

19. **Theorem:** Centralizer of '*a*' in *G* is a subgroup of *G*.

20. **Integral powers of an element of a group:** Suppose *G* is a group and the composition has been denoted multiplicatively, let $a \in G$. Then by closure property *a*, *aa*, *aaa*, ... etc. are all elements of *G*. Since the composition in *G* obeys associative law, therefore, *aaa*... *a* to *n* factors is independent of the manner in which the factors may be grouped.

If *n* is positive integer, we define $a^n = \underbrace{aaa.....a}_{n \text{ times}}$ to *n* factors. If *e* is the identity element of the group *G*, then we define $a^0 = e$.

Also, we define $a^{-n} = (a^n)^{-1}$ where $(a^n)^{-1}$ is the inverse of a^n in *G*.

$$a^{-n} = (a^n)^{-1} = \underbrace{(aaa.....a)^{-1}}_{n \text{ times}} = \underbrace{a^{-1}.a^{-1}.a^{-1}......a^{-1}}_{n \text{ times}} = (a^{-1})^n \; .$$

Thus, $a^{-n} = (a^n)^{-1} = (a^{-1})^n$

21. **Theorem** : For any element '*a*' of a group *G* the set $<a> = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of the group *G*.

Proof: Since $a \in <a> \Rightarrow <a>$ is non empty.

Let $a^n, a^m \in <a>$. Then $a^n (a^m)^{-1} = a^{n-m} \in <a>$

So $a^n, a^m \in <a> \Rightarrow a^n (a^m)^{-1} \in <a>$

Hence <*a*> is a subgroup of *G*.

SOME KEY FACTS

1. Order of identity element is one and only identity element is of order one.

2. Order of group is finite $\Rightarrow$ order of each element is finite.

3. Order of each element finite $\not\Rightarrow$ order of group finite.

Ex. $(P(\mathbb{N}), \Delta)$ The power set of all natural numbers with symmetric difference make a group which has all elements of order 2 but group itself is infinite.

4. Let a, b, x are elements of a group G and $o(a)$ and $o(b)$ is finite then

(*i*) $o(a) = o(a^{-1})$

(*ii*) $o(a) = o(x^{-1} a\, x)$

(*iii*) $(x^{-1} a\, x)^k = x^{-1}\, a^k\, x$

(*iv*) $o(ab) = o(ba)$

(*v*) In general $o(ab) \neq o(a) \cdot o(b)$

(*vi*) If $ab = ba,\ g.c.d.\big(o(a), o(b)\big) = 1$ then $o(ab) = o(a) \cdot o(b)$

5. Every even order group has even number of self inverse element.

6. Every even order group has odd number of element of order 2.

PROPERTIES ON SUBGROUP

7. Arbitrary intersection of subgroups of a group is also a subgroup.

8. Union of subgroup of a group may or may not be subgroup.

9. Union of subgroup of a group is subgroup iff one is contained in other.

10. Product of two subgroup of group may or may not be subgroup.

11. *H* and *K* are two subgroups of a group *G*, $HK = \{h\,k : h \in H, k \in K\}$ is subgroup iff $HK = KH$.

12. *H* and *K* are abelian subgroups of a group *G* then *H K* is always a subgroup.

13. *H* and *K* are subgroup of *G*, then $o(HK) = \dfrac{o(H) \cdot o(K)}{o(H \cap K)}$.

Note that *HK* is always subset of *G* but subgroup may or may not.

14. $H, K < G$ s.t. $o(H) > \sqrt{o(G)},\ o(K) > \sqrt{o(G)} \Rightarrow o(H \cap K) > 1$ (non-trivial subgroup)

15. Let *H* be a subgroup of *G* then (*i*) $H^{-1} = \{h^{-1} : h \in H\} = H$

(*ii*) $HH = H$

16. *H* be a finite subset of group *G* such that $H\ H = H \Rightarrow H$ subgroup of *G*.

17. The centre of group *G* is subgroup $G,\ Z(G) < G$

18. Normalizer of a group *G* is subgroup of $G,\ N(a) < G,\ \forall\ a \in G$

19. *G* be group then

(*i*) $Z(G) = \bigcap\limits_{\forall\ a \in G} N(a)$

(*ii*) *Z*(*G*) is subgroup of $N(a),\ \forall\ a \in G$

SOME IMPORTANT GROUPS AND THEIR PROPERTIES

1. $(\mathbb{Z},+)$ the set of integers under addition

(*i*) is an infinite cyclic group.

(*ii*) Has exactly two generators $\{1, -1\}$.

(*iii*) Identity element is only element is of finite order i.e. every non-identity element is of infinite order.

(*iv*) It has infinite subgroups $\{n\mathbb{Z} : n \in \mathbb{Z}\}$.

(*v*) It has exactly one subgroup of finite order $\{0\}$.

(*vi*) It has infinite subgroup of infinite order

2. $(\mathbb{C}^*, \bullet)$ the set of non-zero complex numbers under multiplication

(*i*) Non-cyclic abelian group of infinite order.

(*ii*) $\forall\ n \in \mathbb{N}, \exists$ an element of each finite order *n* i.e. it has an element of each finite order.

(*iii*) It has infinite number of elements of finite order.

(*iv*) It has infinite number of elements of infinite order.

(*v*) It has infinite number of subgroups of finite order.

(*vi*) It has infinite number of subgroups of infinite order.

(*vii*) If $z \in \mathbb{C}^*$ is of finite order then $|z| = 1$.

(*viii*) $\forall\ n \in \mathbb{N}, \exists$ exactly $\phi(n)$ element of order *n*.

(*ix*) $\forall\ n \in \mathbb{N}, \exists$ exactly one cyclic subgroup of order *n*.

(*x*) It has countable number of elements of finite order.

(*xi*) Every element $z \in \mathbb{C}^*$ such that $|z| \neq 1$ is of infinite order.

3. $(\mathbb{R}^*, \bullet)$ the set of non-zero real numbers under multiplication

(*i*) It is non-cyclic abelian group of infinite order.

(*ii*) 1 and –1 are only element of finite order.

(*iii*) It has exactly two subgroups of finite order.

(*iv*) Has unique proper subgroup of finite order.

(*v*) Infinite number of subgroup of infinite order.

4. $(P(\mathbb{N}), \Delta)$ the power set of natural numbers under symmetric difference

(*i*) It is an infinite non-cyclic abelian group.

(*ii*) Every elements is self inverse.

(*iii*) It is a group of infinite order in which every non-identity element is of order two.

(*iv*) It has infinite number of subgroups of order two.

(*v*) It has infinite number of subgroups of order 2^n, for each $n \in \mathbb{N}$

(*vi*) If H be finite order subgroup then $o(H) = 2^n$ for some n.

(*vii*) There does not any subgroup of odd order which is proper.

(*viii*) It has infinite number of infinite order subgroups

5. The set $\mathbb{Z}_n = \{0, 1, 2, ...n-1\}$ where n is a positive integer form a finite cyclic group under the composition of addition module n $(+_n)$

(*i*) The number of generators in $\mathbb{Z}_n$ are $\phi(n)$.

(*ii*) If k/n then there is unique subgroup of order k.

(*iii*) The number of subgroups in $\mathbb{Z}_n$ are $\tau(n)$.

(*iv*) The number of proper subgroup in $\mathbb{Z}_n$ are $\tau(n) - 2$.

(*v*) If k/n then number of elements of order $k = \phi(k)$.

6. The set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ form a finite non-abelian group, where $i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,$ $ki = j,\ ji = -k, kj = -i, ik = -j$

(*i*) It is a non-abelian group is called Quaternion group and is generally denoted by Q_8.

(*ii*) It has 6 elements of order 4, one element of order 2 and one identity element.

(*iii*) It has 6 subgroups. 3 subgroups of order 4, one is of order 2, two improper subgroup.

(*iv*) It's every proper subgroup is cyclic/abelian but group itself is non-abelian.

Remarks :

It is very useful to give a counter example in many concepts.

7. The set $K_4 = \{e, a, b, c\}$ form a finite abelian group of order 4, where $ab = c = ba,\ bc = a = cb,$ $ca = b = ac$ and $a^2 = b^2 = c^2 = e$.

(*i*) It is an abelian group is called Klein's group and is generally denoted by K_4.

(*ii*) Least order non-cyclic group.

(*iii*) Every element is self inverse.

(*iv*) Every non-identity element is of order 2.

(*v*) It has three subgroup of order two and two improper subgroup.

(*vi*) Group itself non-cyclic but every proper subgroup is cyclic.

8. The set $U(n) = \{x : x \in \mathbb{N} \text{ s.t. } 1 \le x < n \text{ and g.c.d.}(x, n) = 1\}$ under the operation of multiplication modulo $n, (\times_n)$,

(*i*) Finite abelian group for each $n \in N$.

(*ii*) Order of $U(n)$ is $\phi(n)$ {Euler's ϕ function}.

(*iii*) $U(n), \forall\ n \ge 3$ has even number of self-inverse elements.

(*iv*) $U(n), \forall\ n \ge 3$ always has an element of order 2, hence it always has a subgroup of order 2.

(*v*) $U(n), \forall\ n \ge 3$ always has odd number of elements of order 2, hence it always has *n* odd number of subgroup of order 2.

(*vi*) It is cyclic group if $n = p^k$ (p is odd prime)

9. Let $GL\ (n, F)$ be the set of $n \times n$ matrices with non-zero determinant with entries in the field F.

(*i*) $GL\ (n, F)$ is an infinite order group with matrix multiplication if field is infinite.

(*ii*) It is a non-abelian group $\forall\ n > 1$ and F is non-trivial field.

(*iii*) $o\left[GL\,(n, \mathbb{Z}_p)\right] = (p^n - p^{n-1})\,(p^n - p^{n-2})...(p^n - 1)$

10. Let $SL\,(n, F)$ be the set of $n \times n$ matrices with determinant 1 with entries in the field *F*.

(*i*) It is an infinite order group with M.M if field is infinite.

(*ii*) It is a non-abelian group $\forall\, n > 1$ and *F* is non-trivial field.

(*iii*) $SL\,(n, F)$ is a proper subgroup of $G\,L\,(n, F)$

(*iv*) $o\left[SL\,(n, \mathbb{Z}_p)\right] = \dfrac{(p^n - p^{n-1})\,(p^n - p^{n-2}) ... (p^n - 1)}{p-1}$

11. Dihedral Group :-- A dihedral group is generated by two elements one of order 2 and one of order *n* with special relation and denoted by D_{2n}. Its generator and relation are given by and it is defined as

$$D_{2n} = \left\{x^i y^j : i = 0, 1,\ j = 1, 2, ..., n-1,\ x^2 = e,\ y^n = e,\ xy = y^{-1}x\right\}$$

(*i*) D_{2n} is non-abelian group of order 2*n*.

(*ii*) D_{2n} has *n* elements of order 2 if *n* is odd.

(*iii*) D_{2n} has *n* + 1 elements of order 2 if *n* is even.

(*iv*) Largest possible order of any element in D_{2n} is *n*.

(*v*) For every *d* | *n* and $d \neq 2$, D_{2n} has exactly $\phi(d)$ element of order *d*.

(*vi*) For every *d* | *n*, ∃ a cyclic subgroup of order *d* in D_{2n}.

(*vii*) Total number of subgroups of $D_{2n} = \tau(n) + \sigma(n)$

where $\tau(n)$ - number of positive divisors of *n*.

$\sigma(n)$ - sum of all positive divisors of *n*.

Solved Examples

1. Let *G* be the group of all 2 × 2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ under matrix multiplication, where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3. The order of *G* is **[D.U. 2016]**

(a) 24 (b) 16 (c) 48 (d) 81

Soln. If $G = \left\{A = \left[a_{ij}\right]_{n\times n} \mid \det\,(A) \neq 0 \text{ and } a_{ij} \in \mathbb{Z}_p\right\}$, then

$$o(G) = \left(p^n - 1\right)\left(p^n - p\right).....\left(p^n - p^{n-1}\right)$$

Given $n = 2$ and $p = 3$

$$\Rightarrow o(G) = \left(p^2 - 1\right)\left(p^2 - p\right)$$

$$= \left(3^2 - 1\right)\left(3^2 - 3\right) = 48$$

Hence correct option is (c)

2. Let $G = \{a_1, a_2, ...a_{25}\}$ be a group of order 25. For $b, c \in G$ let **[D.U. 2018]**

$bG = \{ba_1, ba_2, ..., ba_{25}\}, Gc = \{a_1c, a_2c, ..., a_{25}c\}$. Then

(a) $bG = Gc$ only if $b = c$

(b) $bG = Gc\ \forall b, c \in G$

(c) $bG = Gc$ only if $b^{-1} = c$

(d) $bG \neq Gc$, if $b \neq c$

Soln. $G=\{a_1,a_2,a_3,....,a_{25}\}$

$bG=\{ba_1,ba_2,.....,ba_{25}\}$ for some $b\in G$

Let $ba_i=ba_j$

$\Rightarrow b^{-1}ba_i=b^{-1}ba_j$

$\Rightarrow a_i=a_j$

$\Rightarrow$ all the elements of bG are distinct.

Also $|bG|=25$ and $bG\subseteq G$ (By closure property)

$\Rightarrow bG=G$

Similarly we can prove $Gc=G$

$\Rightarrow bG=Gc\ \forall b,c\in G$

Hence correct option is (b)

3. Let *n* be the order of an element *a* of a group *G*. Then which of the following elements of *G* has order different from *n* ?

(a) a^p, where *p* is relatively prime to *n* (b) $x^{-1}ax$, where $x\in G$

(c) a^{-1} (d) ax, where $x\in G$ **[B.H.U.-2011]**

Soln. Given, $o(a)=n$

$$o(a^p)=\frac{o(a)}{(p,n)}=o(a)$$

$\Rightarrow o(a^p)=o(a)$

Also, we know that $o(a)=o(a^{-1})=o(xax^{-1})\ \forall x\in G$

$\Rightarrow$ Correct option is (d)

4. Let $\mathbb{Z}$ denote the set of integers. Which of the following operations on $\mathbb{Z}$ gives a group ?

(a) $a*b=ab$ (b) $a*b=a-b$ (c) $a*b=a+b-ab$ (d) $a*b=a+b+1$

where $a,b\in\mathbb{Z}$ **[B.H.U.-2015]**

Soln. For option (a)

$\mathbb{Z}$ is not a group under binary operation $a b = a b$ since it does not satisfy the inverse property.

For option (b)

$\mathbb{Z}$ is not a group under binary operation $a b = a - b$ since it does not satisfy the associate property

For option (c)

$\mathbb{Z}$ is not a group under binary operation $a b = a + b - a b$, since $1\in\mathbb{Z}$ does not have inverse.

For option (d)

$\mathbb{Z}$ is a group under binary operation $ab= a+b+1$, since it satifies all the properties of a group.

Hence correct opration is (d)

5. If a, b are any two elements of a group $(G, \bullet)$ such that $o(ab^{-1}) = 10$, then $o(b^{-2}ab)$ is equal to

(a) 30 (b) 20 (c) 10 (d) 5 **[B.H.U.-2015]**

Soln. Given $o\left(ab^{-1}\right)=10$

We know that

$o\left(xax^{-1}\right)=o\left(a\right) \; \forall \; x \in G; a \in G$

and $o\left(ab\right)=o\left(ba\right) \forall a, b \in G$

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

Also $o\left(b^{-1}a\right)=o\left(b^{-1}\left(b^{-1}a\right)b\right)$ (taking $x=b^{-1}$)

$o\left(b^{-1}\left(b^{-1}a\right)b\right)=o\left(b^{-2}ab\right)=10$

Hence correct option is (c)

6. Let $(G, \bullet)$ be a group. Which of the following is not a subgroup of G ?

(a) $\{x \in G : ax = xa\}$, where a is a fixed element of G **[B.H.U.-2015]**

(b) $\{x \in G : xH = Hx\}$, where H is a subgroup of G

(c) $\{x \in G : x^2 = e\}$, where e is the identity of G

(d) $\{x \in G : x \in H_1$ or $x \in H_2\}$, where H_1, H_2 are subgroups of G

Soln. $\left\{x \in G : x \in H_1 \text{ or } x \in \mathrm{H}_2\right\} = H_1 \cup H_2$

We know that it H_1 and H_2 are two subgroups of a group G then $H_1 \cup H_2$ is a subgroup of G iff either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

$\Rightarrow H_1 \cup H_2$ is not always a subgroup of G.

Hence correct option is (d)

7. The solutions of $x^2 + x + 4 = 0$ in $\mathbb{Z}_6$ are : **[B.H.U.-2016]**

(a) 1, 4 (b) 2, 4 (c) 1, 3 (d) 0, 1

Soln. Clearly 1 and 4 satisfies the equation $x^2 + x + 4 = 0$ and 0, 2, 3 donot.

Hence, correct option is (a)

8. If the order of every element of a group is 2, then this group **[B.H.U-2018]**

(a) is Abelian (b) is cyclic (c) is of infinite order (d) is definitely non-Abelian

Soln. If the order of every non- identity element in a group is 2, then this group is always abelian.

$\therefore (ab)^{-1} = ab$

$\Rightarrow b^{-1} a^{-1} = ab \Rightarrow ba = ab$

Hence correct option is (a)

9. If a is an element of a group G such that $o(a) = n = 2m$, then which one of the following is also of order n?

(a) a^2 (b) a^m (c) a^4 (d) a^3

Soln. We know that if $o(G) = n,$ then $o(a) = o(a^p)$ iff $(n, p) = 1$

Here $(n, p) = 1$

$o(a) = n = 2m$

Also $(3, 2m) = 1$

Hene correct option is (d)

10. The order of the smallest possible non-trivial group containing elements x and y such that $x^7 = y^2 = e$ and $yx = x^4 y$ is

(a) 1 (b) 2 (c) 7 (d) 14

Soln. Given, $x^7 = y^2 = e$ and $yx = x^4 y$

Let $\mathbb{Z}_2 = \{e, a\}$

Take $x = e, y = a$

$\Rightarrow$ Satisfies all the properties

Hence correct option is (b).

11. Let G be a group of order 231. The number of elements of order 11 in G is

(a) 11 (b) 12 (c) 10 (d) 13

Soln. The number of elements of order n in G is a multiple of $\phi(n)$

Here $o(G) = 231$

The number of elements of order 11 in G is multiple of $\phi(11)$ $i.e. 10, 20, 30 ....$

$\Rightarrow$ **Hence correct option is (c)**

12. Let $G = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}$ with $o(x) = 4, o(y) = 2$ and $xy = yx^3$. Then, the number of elements in the center of the group G is equal to

(a) 1 (b) 2 (c) 4 (d) 8

Soln. Given $G = \{e, x, x^2, x^3, y, xy, x^2y, x^3y\}$ here $o(x) = 4, o(y) = 2$ and $xy = yx^3 = yx^{-1}$

$\Rightarrow G = D_4$

The number of elements in the centre of the group $D_n = \begin{cases} 2 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is order} \end{cases}$

Hence correct option is (b)

13. Let G be a group and $a \in G$ be a unique element of order n where $n > 1$. Let $Z(G)$ denote the centre of the group G. Then

(a) $o(G) = n$ (b) $o(Z(G)) > 1$ (c) $Z(G) = G$ (d) $G = S_2$

Soln. Given $a \in G$ is a unique element of order n where $n > 1$

$\Rightarrow$ order of a is 2 and it is unique.

$\Rightarrow a \in Z(G)$

$\Rightarrow o(Z(G)) > 1$

Hence correct option is (b)

14. Let G be a group and $a, b \in G$. If $a^{17} = b^{17}$ and $a^{30} = b^{30}$ then

(a) $a = b$ (b) $ab = ba$ and $o(a) \neq o(b)$

(c) $a = b^{-1}$ and $o(a) \neq o(b)$ (d) $o(a) = o(b)$ and $a \neq b$

Soln. $a^{30} = b^{30}$ and $a^{17} = b^{17}$

$\Rightarrow a^{-30} = b^{-30}$ and $a^{34} = b^{34}$

$\Rightarrow a^{34} = b^{34}$

$\Rightarrow a^{-30}a^{34} = a^{-30}b^{34} = b^{-30}b^{34}$

$\Rightarrow a^{4} = b^{4}$

$\Rightarrow a^{16} = b^{16}$

$\Rightarrow a^{-16} = b^{-16}$

Given $a^{17} = b^{17}$

$\Rightarrow a^{-16}a^{17} = a^{-16}b^{17} = b^{-16}b^{17}$

$\Rightarrow a = b$

Hence correct option is (a)

15. Let $x \in \mathbb{R} - \{0\}$ then the correct statement is:

(a) If $x^2 \in \mathbb{Q}$ then $x^3 \in \mathbb{Q}$ (b) If $x^3 \in \mathbb{Q}$ then $x^2 \in \mathbb{Q}$

(c) If $x^2 \in \mathbb{Q}$ and $x^4 \in \mathbb{Q}$ then $x^3 \in \mathbb{Q}$ (d) If $x^2 \in \mathbb{Q}$ and $x^5 \in \mathbb{Q}$ then $x \in \mathbb{Q}$

Soln. For option (a)

Let $x = \sqrt{2}$

Clearly $x^2 = 2 \in \mathbb{Q}$

But $x^3 = 2^{3/2} \notin \mathbb{Q}$

For option (b)

Let $x = 2^{1/3}$

Clearly $x^3 = 2 \in \mathbb{Q}$

But $x^2 = x^{2/3} \notin \mathbb{Q}$

For option (c)

Let $x = \sqrt{2}$

Clearly $x^2 = 2 \in \mathbb{Q}$ and $x^4 = 2^2 \in \mathbb{Q}$

But $x^3 = 2^{3/2} \notin \mathbb{Q}$

For option (d)

Given $x^2 \in \mathbb{Q} \Rightarrow x^{-2} \in \mathbb{Q}$ ($\because$ $\mathbb{Q} - \{0\}$ is closed) w.r.t multiplication

Now $x^5 \in \mathbb{Q}$

$\Rightarrow x^{-2}x^{-2}x^{5} \in \mathbb{Q}$

$\Rightarrow x \in \mathbb{Q}$

Hence correct option is (d)

16. Let $\mathbb{Q}$ be the set of rationals and define a binary operation on $\mathbb{Q}$ by $a*b$ =a+b $-ab$. Then

(a) $(\mathbb{Q},*)$ is a group (b) $(S,*)$ is a group for some subset $S \subseteq \mathbb{Q}$ **[H.C.U-2017]**

(c) $(\mathbb{Q},*)$ is not associative (d) $(\mathbb{Q},*)$ has no identity.

Soln. We can easily check that $(\mathbb{Q},*)$ is closed associative and has identity 0.

To check inverse:

Let $a \in \mathbb{Q}$

Let $b \in \mathbb{Q}$ be the inverse of a

$\Rightarrow a+b-ab=0$

$\Rightarrow a+b(1-a)=0$

$\Rightarrow a=b(a-1)$

$\Rightarrow b=\dfrac{a}{a-1}$

$\Rightarrow a \neq 1$

$\Rightarrow (S,*)$ is group for some subset $S \subseteq \mathbb{Q}$

Hence correct option is (b)

17. Consider the following two statements

S_1 : There cannot exist an infinite group in which every element has a finite order. **[H.C.U-2015]**

S_2 : In a group G if $a \in G,\ a^7=e$ and $a^9=e,$ then $a=e$

Which of the following statements is true?

(a) Both S_1 and S_2 are true (b) Both S_1 and S_2 are false

(c) S_1 is false but S_2 are true (d) S_1 is true but S_2 are false

Soln. S_1: Let $G=(P(\mathbb{N}),\Delta)$

Now G is an infinite group, but every element of G has finite order.

S_2 : Given $a^7=e$ and $a^9=e$

$\Rightarrow o(a)\,|\,7$ and $o(a)\,|\,9$

Now $a^{-7}a^{9}=a^{-7}e \quad (\because a^7=e \Rightarrow a^{-7}=e)$

$\Rightarrow\ a^{-7}a^{9}=a^{-7}e$

$\Rightarrow\ a^{2}=e$

$\Rightarrow\ o(a)\,|\,2$

$\Rightarrow$ Either $o(a)=1$ or $o(a)=2$

If $o(a)=2$ then 2 does not divides 7 and 9

$\Rightarrow o(a)=1$

$\Rightarrow a=e$

Hence correct option is (c)

18. Let G be a group and $a,b\in G$ such that $o(a)=6, o(b)=2$ and $a^3b=ba$. Then $o(ab)$ is

(a) 6 (b) 8 (c) 12 (d) 2 **[H.C.U-2018]**

Soln. Given $o(a)=6, o(b)=2$ and $a^3b=ba$

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

$=a(a^3b)b=a^4b^2$

$=a^4\,(\because b^2=e)$

$(ab)^3=a^4(ab)=a^5b$

$(ab)^4=(a^5b)(ab)$

$=a^5(ba)b=a^5a^3bb$

$=a^8b^2=a^2$

$(ab)^5=a^2(ab)=a^3b$

$(ab)^6=(a^3b)(ab)=a^3(ba)b$

$=a^3a^3bb=e$

$\Rightarrow o(ab)=6$

Hence correct option is (a)

19. Let G be a group and let H and K be two subgroups of G. If both H and K have 12 elements, which of the following numbers cannot be the cardinality of the set $HK=\{hk:h\in H, k\in K\}$?

(a) 72 (b) 60 (c) 48 (d) 36 **[TIFR-2014]**

Soln. Given $o(H)=o(K)=12$

We know that $o(HK)=\dfrac{o(H)\cdot o(K)}{o(H\cap K)}$

$\Rightarrow\; o(HK)o(H\cap K)=o(H)o(K)$

$\Rightarrow\; o(HK)\,|\,o(H)o(K)$

$\Rightarrow\; o(HK)\,|\,144$

Now $60 \nmid 144$

Hence correct option is (b)

20. Let H_1, H_2 be two distinct subgroups of a finite group G, each of order 2. Let H be the smallest subgroup containing H_1 and H_2. Then the order of H is **[TIFR-2014]**

(a) always 2 (b) always 4 (c) always 8 (d) none of the above

Soln. Let $G=S_3$

Let $H_1=\{I,(12)\}$ and $H_2=\{I,(23)\}$

If H_1 and H_2 are distinct subgroups of G each of order 2. But S_3 is the smallest subgroup of S_3 containing both H_1 and H_2. Also $o(S_3)=6$

Hence correct option is (d)

21. Let A be the 2 × 2 matrix $\begin{pmatrix} \sin\frac{\pi}{18} & -\sin\frac{4\pi}{9} \\ \sin\frac{4\pi}{9} & \sin\frac{\pi}{18} \end{pmatrix}$. Then the smallest number $n\in\mathbb{N}$ such that $A^n = I$ is

(a) 3 (b) 9 (c) 18 (d) 27 **[TIFR-2015]**

Soln. Given $A=\begin{pmatrix} \sin\frac{\pi}{18} & -\sin\frac{4\pi}{9} \\ \sin\frac{4\pi}{9} & \sin\frac{\pi}{18} \end{pmatrix}$

$$\Rightarrow A=\begin{pmatrix} \sin\left(\frac{\pi}{2}-\frac{4\pi}{9}\right) & -\sin\frac{4\pi}{9} \\ \sin\frac{4\pi}{9} & \sin\left(\frac{\pi}{2}-\frac{4\pi}{9}\right) \end{pmatrix}$$

$$\Rightarrow A=\begin{pmatrix} \cos\frac{4\pi}{9} & -\sin\frac{4\pi}{9} \\ \sin\frac{4\pi}{9} & \cos\frac{4\pi}{9} \end{pmatrix}$$

Clearly A is an orthogonal matrix

Now $A^9=\begin{pmatrix} \cos\frac{4\pi}{9} & -\sin\frac{4\pi}{9} \\ \sin\frac{4\pi}{9} & \cos\frac{4\pi}{9} \end{pmatrix}^9$

$$=\begin{pmatrix} \cos 4\pi & -\sin 4\pi \\ \sin 4\pi & \cos 4\pi \end{pmatrix}$$

$$\Rightarrow A^9=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence correct option is (b)

22. Which of the following form a group ?

(a) $G=\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} : a\in\mathbb{R}, a\neq 0\right\}$ with respect to matrix multiplication. **[NBHM-2009]**

(b) $\mathbb{Z}_4$, the set of all integers modulo 4, with respect to multiplication.

(c) $G=\{f:[0,1]\to\mathbb{R}\,;\, f$ is continuous$\}$ with respect to the operation defined by $(f\cdot g)(x) = f(x)\,g(x)$ for all $x\in[0,1]$.

Soln. For option (a)

Given $G=\left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix}; a\in\mathbb{R}, a\neq 0\right\}$

Let $A, B\in G$

$\Rightarrow A=\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ and $B=\begin{pmatrix} b & b \\ b & b \end{pmatrix}$ for some $a,b\in\mathbb{R}-\{0\}$

Now, $AB=\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix}$

$$AB=\begin{pmatrix} ab+ab & ab+ab \\ ab+ab & ab+ab \end{pmatrix}=\begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}\in G$$

$\Rightarrow G$ is closed with respect to multiplication.

Also we know that matrix multiplication is associative.

Let I be the identity of G.

$\Rightarrow I=\begin{pmatrix} e & e \\ e & e \end{pmatrix}$ for some $e\in\mathbb{R}-\{0\}$

$\Rightarrow AI=IA=A\ \forall A\in G$

$\Rightarrow\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix}=\begin{pmatrix} a & a \\ a & a \end{pmatrix}\ \forall\, a\in\mathbb{R}-\{0\}$

$\Rightarrow\begin{pmatrix} 2ae & 2ae \\ 2ae & 2ae \end{pmatrix}=\begin{pmatrix} a & a \\ a & a \end{pmatrix}$

$\Rightarrow e=\frac{1}{2}$

Hence identity is $I=\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

If $A=\begin{pmatrix} a & a \\ a & a \end{pmatrix}; a\neq 0$ then $\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$ is the inverse of A.

Hence G is a group with respect to matrix multiplication

For option (b):

Clearly $2\in\mathbb{Z}_4$ and 2 does not have inverse in $\mathbb{Z}_4$

For option (c)

Zero function $\in G$, but it does not have inverse

$\Rightarrow G$ is not a group

Hence correct option is (a)

23. From the following subgroups of $GL_2(\mathbb{C})$, pick out those which are abelian: **[NBHM-2011]**

(a) The subgroup of invertible upper triangular matrices.

(b) The subgroup S defined by $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R}, \text{ and } |a|^2 + |b|^2 = 1 \right\}$.

(c) The subgroup U defined by $U = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}; a, b \in \mathbb{C}, \text{ and } |a|^2 + |b|^2 = 1 \right\}$.

Soln. For option (a)

Let $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}$

Clearly $A, B \in GL_2(\mathbb{C})$ and A, B is uppertriangular matrix.

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 11 \\ 0 & 12 \end{bmatrix}$$

$$BA = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 13 \\ 0 & 12 \end{bmatrix}$$

Clearly $AB \neq BA$

$\Rightarrow$ option (a) is not true

$\Rightarrow$ The subgroup of invertible upper triangular matrices is not abelian.

For option (b):

Given $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}; a, b \in \mathbb{R} \text{ and } |a|^2 + |b|^2 = 1 \right\}$

Let $A, B \in S$

$\Rightarrow A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$; $a, b, c, d \in \mathbb{R}$ and $|a|^2 + |b|^2 = 1$ and $|c|^2 + |d|^2 = 1$

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{pmatrix}$$

$$BA = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}$$

$\Rightarrow AB = BA$

$\Rightarrow S$ is an abelian subgroup.

Similarly we can check U is not an abelian subgroup.

Hence correct option is (b)

24. Let G be an group and $a, b \in G$. Then which one of the following statements is not true ? **[CUCET-2016]**

(a) If a, b and ab have same order $ab = ba$

(b) If $a^3 = e$, the identity element of G and $aba^{-1} = b^2$ then the order of b can't be 16

(c) ab and ba have same order

(d) b and aba^{-1} have same order.

Soln. For option (a)

Let $G = Q_8$

Let $a = i, b = j$

Clearly $o(a) = o(b) = 4$

$ab = ij = k$

$\Rightarrow o(ab) = 4$

Now $ba = ji = -k$

$\Rightarrow ab \neq ba$

Hence statement (a) is false

Hence correct option is (a)

25. Let $G = \{(a,b) \in \mathbb{R}^2 \mid a \neq 0\}$. Define a binary operation on G by (a,b) . $(c, d) = (ac, bc + d)$.With respect to this operation on G, which one of the following is true ? **[CUCET-2016]**

(a) G is a group with identity (1, 1) and inverse of (a, b) is (a^{-1}, ba^{-1}).

(b) G is a group with identity (1,1) and inverse of (a, b) is $(a^{-1}, -ba^{-1})$.

(c) G is a group with identity (1,0) and inverse of (a, b) is $(a^{-1}, -ba^{-1})$.

(d) G is not a group

Soln. Given $G = \{(a,b) \in \mathbb{R}^2 \mid a \neq 0\}$

Also $(a,b)(c,d) = (ac, bc + d)$

Clearly G is closed

Let $x, y, z \in G$

$\Rightarrow x = (a,b), y = (c,d)$ and $z = (e, f); a,b,c,d,e, f \in \mathbb{R}$ and $a \neq 0, c \neq 0, e \neq 0$

Now $(xy)z = ((a,b)(c,d))(e, f)$

$= (ac, bc + d)(e, f)$

$= (ace, (bc + d)e + f)$

$x(yz) = (a,b)((c,d)(e, f))$

$= (a,b)(ce, de + f)$

$= (ace, bce + de + f)$

$\Rightarrow (xy)z = x(yz) \ \forall \ x, y, z \in G$

Associative property hold in G.

Let $(e_1, e_2) \in G$ be the identity of G where $e_1, e_2 \in \mathbb{R}$ and $e_1 \neq 0$

$\Rightarrow (a,b)(e_1,e_2) = (a,b) \quad \forall \ (a,b) \in G$

$\Rightarrow (ae_1, be_1 + e_2) = (a,b)$

$\Rightarrow e_1 = 1$ and $e_2 = 0$

$\Rightarrow (1,0)$ is the identity of G.

Let (c,d) be the inverse of (a,b)

$\Rightarrow (a,b)(c,d) = (1,0)$

$\Rightarrow (ac, bc + d) = (1,0)$

$ac = 1$ and $bc + d = 0$

$c = \frac{1}{a}$ and $d = \frac{-b}{a}$

Hence correct option is (c)

26. Which one of the following subsets of G, given in the above problem is not a subgroup of G ?

(a) $H_1 = \{(1,0)\}$ **[CUCET-2016]**

(b) $H_2 = \{(a,b) \in G : a = 1\}$

(c) $H_3 = \{(a,b) \in G : a \text{ is rational}\}$

(d) $H_4 = \{(a,b) \in G : a \text{ is irrational}\}$

Soln. For option (d)

Given $H_4 = \{(a,b) \in G : a \text{ is irrational}\}$

Let $(\sqrt{2},1) \in G$

Now $(\sqrt{2},1)(\sqrt{2},1) = (2, \sqrt{2}+1) \notin H_4$

$\Rightarrow H_4$ is not a subgroup of G.

Hence correct option is (d)

27. Let G be a finite group of even order. Then which of the following statements is correct ?

(a) The number of elements of order 2 in G is even **[ISI-2018]**

(b) The number of elements of order 2 in G is odd

(c) G has no subgroup of order 2.

(d) None of the above

Sonl. We know that if G is a finite group of even order then number of elements of order 2 in G is always odd.

Hence correct option is (b)

28. Let p be a prime number. Consider the group $SL(2,\mathbb{Z}_p)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\middle| a,b,c,d\in\mathbb{Z}_p \text{ and } ad-bc=1\right\}$

under the matrix multiplication. Then the order of $A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z}_p)$ is **[H.C.U-2018]**

(a) ∞ (b) p (c) 1 (d) $p-1$

Soln. Given $A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$$A^2=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$A^3=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

Continuing like this, we have

$$A^p=\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow o(A)=p$$

Hence correct option is (b)

29. Which of the following form a group under matrix multiplication ?

(a) $\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix}: a\neq 0, a\in\mathbb{R}\right\}$

(b) $\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix}: |a|+|b|\neq 0, a,b\in\mathbb{R}\right\}$

(c) $\left\{\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}: \theta\in[0,2\pi]\right\}$ **[NBHM-2012]**

Soln. For option (a)

Given $G=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix}; a\neq 0, a\in\mathbb{R}\right\}$

G is a group under matrix multiplication with identity $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$ and inverse of $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ is $\begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix}$

For option (b):

Given $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : |a| + |b| \neq 0, a, b \in \mathbb{R} \right\}$

Let $A, B \in G$

$\Rightarrow A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$, where $a,b,c,d \in \mathbb{R}$ and $|a| + |b| \neq 0$, $|c| + |d| \neq 0$

$$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{bmatrix}$$

Also $|AB| = (ac - bd)^2 + (ad + bc)^2$

$= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd$

$= a^2(c^2 + d^2) + b^2(c^2 + d^2)$

$= (a^2 + b^2) \cdot (c^2 + d^2)$

$\Rightarrow |AB| \neq 0$

$\Rightarrow AB \in G$

$\Rightarrow G$ is closed with respect to matrix multiplication

Also matrix multiplication is associative

Clearly $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity of G.

Inverse of $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is $\dfrac{1}{a^2 + b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

$\Rightarrow G$ is a group under matrix multiplication

Similarly we can prove for option (c)

Hence correct option is (a), (b) and (c).

30. Let G be an arbitrary group and let a and b be any two distinct elements of G. Which of the following statements are true ?

(a) If m is the order of a and if n is the order of b, then the order of ab is the l.c.m. of m and n.

(b) The order of ab equals the order of ba

(c) The elements ab and ba are conjugate to each other **[NBHM-2014]**

Soln. For option (a)

We know that if a and b are of finite ordered elements of G then the order of ab need not be finite.

For option (b)

$o(ab)$ is always equal to $o(ba)$

For option (c)

we can write

$ab = abaa^{-1}$

$\Rightarrow ab$ and *ba* are conjugate to each other

Hence correct opiton is (b) and (c)

31. Pick out the true statements:

(a) Every group of order 36 is abelian

(b) A group in which every element is of order at most 2 is abelian **[NBHM-2005]**

Soln. For option (a)

Let $G = D_{18}$

Clearly $o(G) = 36$ and *G* is non abelian

For option (b)

We know that if in a group every element is of order atmost 2. Then group is always abelian

Hence correct option is (b)

32. Which of the following statements are true ?

(a) Any group of order 15 is abelian

(b) Any group of order 25 is abelian

(c) Any group of order 55 is abelian **[NBHM-2005]**

Soln. We know that if *G* is a group of order *pq* where *p* and *q* are distinct primes such that $q > p$ then

(i) if $p \mid (q-1)$ then *G* may not be abelian

(ii) if $p \nmid (q-1)$ then *G* always abelian

Thus any group of order 15 is abelian and group of order 55 may not be abelian

Also every group of order p^2, where *p* is a prime is always abelian

Hence correct option is (a) and (b)

33. Which of the following statements are true ? **[NBHM-2015]**

(a) If *G* is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then *G* is abelian.

(b) If *G* is a group such that $a^2 = e$ for all $a \in G$, where *e* is the identity element in *G*, then *G* is abelian.

(c) If *G* is a group such that $a^2 = e$ for all $a \in G$, where *e* is the identity element in *G*, then *G* is finite.

Soln. For option (a)

We know that if *G* is a group such that $(ab)^2 = a^2b^2 \ \forall a, b \in G$, then *G* is abelian

For option (b):

We know that if $a^2 = e \ \forall a \in G$, then *G* is abelian.

For option (c)

Let $G = (P(\mathbb{N}), \Delta)$

Now $a^2 = a \ \ \forall a \in G;$ but *G* is infinite

Hence correct option is (a), (b)

34. Let G be *a* non-abelian group of order 125. Then the total number of elements in

$Z(G)=\{x\in G : g\,x = x\,g \text{ for all } g\in G\}$ equals_______.

Soln. We know that if G is non abelian group of order p^3, where p is a prime number then $o(Z(G))=5$

Hence correct answer is (5)

35. Let G denote the group of invertible 2 × 2 matrices with entries from $\mathbb{F}_2$ (the group operation being matrix multiplication). What is the order of G ? **[NBHM-2008]**

Soln. Given G = group of invertible 2×2 matrices entries from $\mathbb{F}_2$

$$o(G)=(2^2-1)(2^2-2)=(4-1)(4-2)=6$$

Hence correct answer is (6)

36. Let G be the set of all 2 × 2 symmetric, invertible matrix with real entries then with matrix multiplication G is

(a) an infinite group (b) a finite group (c) not a group (d) an abelian group **[TIFR-2010]**

Soln. Let $A=\begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix}\in G$ as $|A|\neq 0$ and $A=A^T$

$B=\begin{pmatrix}0 & -1\\ -1 & 1\end{pmatrix}\in G$ as $|B|\neq 0$ and $B=B^T$

But $(AB)=\begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix}\begin{pmatrix}0 & -1\\ -1 & 1\end{pmatrix}=\begin{pmatrix}-2 & 1\\ 0 & -2\end{pmatrix}$ is not symmetric.

So G is not closed under matrix multiplication w.r.t. symmetricity.

Hence, correct option is (c).

37. Let I be the set of irrational real number and let $G=I\cup\{0\}$ then under usual addition of real number G is

(a) a group since $\mathbb{R}$ and $\mathbb{Q}$ are group under addition

(b) a group since additive identity is in G

(c) not a group since addition on G is not a binary operation

(d) not a group since not all element in G has an inverse

Soln. As $2+\sqrt{3},\ 2-\sqrt{3}\in G$ but $2+\sqrt{3}+2-\sqrt{3}=4\notin G$. Hence G is not a group as addition on G is not binary operation.

Hence, correct option is (c).

38. Let S be the collection of (isomorphism class of) groups G which have the property that every element of G commutes only with identity element and itself then

(a) $|S|=1$ (b) $|S|=2$ (c) $|S|\geq 3$ and is finite (d) $|S|=\infty$ **[TIFR-2014]**

Soln. $S=\{G\,|\,G=\{e,a\}\ a\neq e\}$ or $S=\{G\,|\,G=\{e\}\}$

$S=\{G\,|\,O(G)=2\}$ or $S=\{\{e\}\}$

in both cases $|S|=1$ as there is only one group of order 2 upto isomorphism $\Rightarrow |S|=1$.

Hence, correct option is (a).

39. If the equation $xyz=1$ holds in a group G does it follow that $yzx=1$. True or false ? **[TIFR-2012]**

Ans. True

Soln. As $x, y, z \in G$ so x^{-1}, y^{-1}, z^{-1} exist in G.

$xyz = 1$

Premultiplying by x^{-1} and post multiply by x on both side we get,

$x^{-1}(xyz)x = x^{-1}(1)x = (x^{-1}x)\,yzx = x^{-1}x$ By associativity

$\Rightarrow yzx = 1.$

Hence true statement.

40. If x, y and z are elements of a group such that $xyz = 1$, then

(a) $yzx = 1$ (b) $yxz = 1$ (c) $zxy = 1$ (d) $zyx = 1$

Soln. If x, y and z are elements of a group such that $xyz = 1$, then $yzx = 1$ and $zxy = 1$.

Hence, correct options are (a) and (c).

41. If H_1 and H_2 are subgroup of a group G then $H_1H_2 = \{h_1 h_2 \in G \mid h_1 \in H_1,\ h_2 \in H_2\}$ is a subgroup of G whether true or false ? **[TIFR-2012]**

Ans. False

Soln. By theorem $H_1 H_2$ is a subgroup of G iff $H_1 H_2 = H_2 H_1$

42. The cardinality of centre of $\mathbb{Z}_{12}$ is

(a) 1 (b) 2 (c) 3 (d) 12

Soln. $G = \mathbb{Z}_{12}$ is abelian

So centre of group = group it self

So cardinality of center of $\mathbb{Z}_{12}$ is 12.

Hence, correct option is (d).

43. Let G be a group and let H and K be two subgroup of G. If both H and K have 12 elements which of the following numbers cannot be the cardinality of the set $HK = \{hk, h \in H, k \in K\}$

(a) 72 (b) 60 (c) 48 (d) 36 **[TIFR-2014]**

Soln. $o(HK) = \dfrac{o(H)\cdot o(K)}{o(H \cap K)}$

$o(H)\,o(K) = 144 = o(HK)\,o(H \cap K)$

If $o(HK) = 72 \Rightarrow o(H \cap K) = \dfrac{144}{72} = 2$. This is possible

If $o(HK) = 60 \Rightarrow o(H \cap K) = \dfrac{144}{60} = 2.4$. This is not possible

Similarly for 48, 36.

Hence, correct option is (b).

44. In the group $(\mathbb{Z}, +)$ the subgroup generated by 2 and 7 is

(a) $\mathbb{Z}$ (b) $5\mathbb{Z}$ (c) $9\mathbb{Z}$ (d) $14\mathbb{Z}$

Soln. Subgroup generated by 2 is $2\mathbb{Z}$ say H

Subgroup generated by 7 is $7\mathbb{Z}$ say K

then subgroup generated by 2 and 7 is $H \cap K\ 2\mathbb{Z} \cap 7\mathbb{Z} = \text{lcm}\,(2, 7)\,\mathbb{Z} = 14\mathbb{Z}$

Hence, correct option is (d).

45. Every countable group G has only countably many distinct subgroups. True or False? **[TIFR-2013]**

Ans. False

Soln. Let G be group consisting of all finite subset of $\mathbb{N}$ with the operation symmetric difference. The group is countably infinite but for each finite or infinite $A \subseteq \mathbb{N}$ there is a subgroup consisting of the finite subset of A. Which are uncountable.

46. Every infinite abelian group has at least one element of infinite order. True or False? **[TIFR-2013]**

Ans. False

Soln. Take $(P(\mathbb{N}), \Delta)$ is an infinite abelian group of infinite order but every element has order two which is not infinite.

47. For a group G, let $F(G)$ denote the collection of all subgroup of G. Which of the following situation can occurs?

(a) G is finite but $F(G)$ is infinite (b) G is infinite but $F(G)$ is finite

(c) G is countable but F(G) is uncountable (d) G is uncountable but $F(G)$ is countable **[TIFR-2014]**

Soln. Same as question 1.

Hence, correct option is (c).

48. There is an element of order 51 in the multiplicative group $(\mathbb{Z}/103\mathbb{Z})^*$ **[TIFR-2013]**

Ans. True

Soln. $G = \mathbb{Z}/103\mathbb{Z} \approx \mathbb{Z}_{103}$

$|G| = \phi(103) = 102$

as G is finite abelian so converse of Langrange's theorem hold as 51 | 102 so there exist an element of order 51 in G.

49. Let $G = \mathbb{Z}/100\mathbb{Z}$ and let $S = \{h \in G \mid o(h) = 50\}$ then $|S|$ equals

(a) 20 (b) 25 (c) 30 (d) 50 **[TIFR-2016]**

Soln. $|G| = 100$ as G is cyclic and 50 | 100 so $|S| = \phi(50) = 50\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 50 \times \frac{1}{2} \times \frac{4}{5} = 20.$

Hence, correct option is (a).

50. Let $U(n)$ be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n. For $n = 248$ the number of element in $U(n)$ is

(a) 60 (b) 120 (c) 180 (d) 240

Soln. $o(U(n)) = \phi(n) = \phi(248) = 248\left(1-\frac{1}{2}\right)\left(1-\frac{1}{31}\right) = 248 \times \frac{1}{2} \times \frac{30}{31} = 120.$

Hence, correct option is (b).

51. Consider $\mathbb{Z}_{24}$ as additive group modulo 24 then the number of elements of order 8 in the group $\mathbb{Z}_{24}$ is

(a) 1 (b) 2 (c) 3 (d) 4

Soln. As $\mathbb{Z}_{24}$ is cyclic group and $o(\mathbb{Z}_{24}) = 24$

Now $8 | 24 \Rightarrow$ Number of elements of order 8 in the group $\mathbb{Z}_{24}$ is $\phi(8) = 8 \times \left(1-\frac{1}{2}\right) = 8 \times \frac{1}{2} = 4$.

Hence, correct option is (d).

52. Let G be a cyclic group of order 6. Then number of elements $g \in G$ such that $G = \langle g \rangle$ is

(a) 5 (b) 3 (c) 4 (d) 2

Soln. $G = \langle g \rangle$ we have to find number of elements of G which generates G. G is cyclic group of order 6 implies that

$G \approx \mathbb{Z}_6$ Hence 1, 5 are generates of G, number of element of G such that $G = \langle g \rangle$ is 2.

Hence, correct option is (d).

53. Let D_8 denote the group of symmetry of square (Dihedral group). The minimal number of generator of D_8 is

(a) 1 (b) 2 (c) 4 (d) 8

Soln. $H = \left\langle x, y \mid x^4 = y^2 = e \right\rangle$ generates D_8

Number of element in H is 2.

Hence, correct option is (b).

54. Which of the following cannot be the class equation of a group of order 10?

(a) $1+1+1+2+5=10$ (b) $1+2+3+4=10$

(c) $1+2+2+5=10$ (d) $1+1+2+2+2+2=10$

Soln. $o(G)$ = 10 = 2 × 5 = $p \times q$. Then $G \approx \mathbb{Z}_{10}$ or D_{10}. So class equation of $\mathbb{Z}_{10} = \underbrace{1+1+1+\cdots+1}_{10\text{ times}}$ and class equation of D_{10} is $1+2+2+5$, so

(i) $1+1+1+2+5$

(ii) $1+2+3+4$

(iii) $1+1+2+2+2+2$ cannot be class equation.

Hence, correct options are (a), (b) and (d).

55. Determine which of the following cannot be the class equation of a group

(a) $10=1+1+1+2+5$ (b) $4=1+1+2$

(c) $8=1+1+3+3$ (d) $6=1+2+3$

Soln. (i) $o(G)=6$ i.e. S_3 $\quad 6=1+2+3$

(ii) $o(G)=10$ (Di-hedral group D_5) $\quad 10=1+2+2+5$

(iii) $o(G)=8$ (Di-hedral group D_4) $\quad 8=1+1+2+2+2$

(iv) $o(G)=4$ (Di-hedral group D_2) $\quad 4=1+1+1+1$

Hence, correct options are (a), (b) and (c).

56. A group G is generated by the elements x, y with the relations $x^3 = y^2 = (xy)^2 = 1$. The order of G is

(a) 4 (b) 6 (c) 8 (d) 12

Soln. By definition of dihedral group it is D_6 i.e., of order 6.

Hence, correct option is (d).

57. Let $A = \begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$ be a matrix over the integers modulo 11. The inverse of A is **[D.U. 2015]**

(a) $A = \begin{pmatrix} 8 & 9 \\ 10 & 9 \end{pmatrix}$ (b) $A = \begin{pmatrix} 10 & 8 \\ 9 & 9 \end{pmatrix}$ (c) $A = \begin{pmatrix} 9 & 10 \\ 9 & 8 \end{pmatrix}$ (d) $A = \begin{pmatrix} 9 & 9 \\ 10 & 8 \end{pmatrix}$

Soln. $A = \begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$ be a matrix over the integers modulo 11. The inverse of A is $A^{-1} = \dfrac{1}{|A|} \cdot \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix}$

$$=\frac{1}{10-18}\begin{pmatrix}5 & 5\\ 8 & 2\end{pmatrix}=\frac{1}{-8}\cdot\begin{pmatrix}5 & 5\\ 8 & 2\end{pmatrix}$$

$$=\frac{1}{3}\cdot\begin{pmatrix}5 & 5\\ 8 & 2\end{pmatrix}=\begin{pmatrix}5/3 & 5/3\\ 8/3 & 2/3\end{pmatrix}=\begin{pmatrix}-6/3 & -6/3\\ -3/3 & -9/3\end{pmatrix}=\begin{pmatrix}-2 & -2\\ -1 & -3\end{pmatrix}$$

$$=\begin{pmatrix}9 & 9\\ 10 & 8\end{pmatrix}$$

Hence, correct option is (d).

58. The order of the group $\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| ad-bc=1 \text{ and } a,b,c,d\in\mathbb{Z}_3\right\}$ relative to matrix multiplication is

(a) 18 (b) 20 (c) 24 (d) 22 **[D.U. 2015]**

Soln. $o(SL(n,\mathbb{Z}_p))=\dfrac{(p^n-1)(p^n-p)...(p^n-p^{n-1})}{(p-1)}$

$$G=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}: ad-bc=1 \text{ and } a,b,c,d\in\mathbb{Z}_3\right\}$$

Given $p=3,\ n=2$

$$o(G)=\frac{(3^2-1)\cdot(3^2-3)}{(3-1)}=\frac{8\times 6}{2}=24$$

Hence, correct option is (c).

59. Let G be the group of all 2×2 matrices $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ under matrix multiplication, where $ad-bc\neq 0$ and a,b,c,d are integers modulo 3. The order of G is

(a) 24 (b) 16 (c) 48 (d) 81 **[D.U. 2016]**

Soln. $o(G)=(p^2-1)\,(p^2-p)=(9-1)\,(9-3)=8\times 6=48.$

Hence, correct option is (c).

60. Let G be a finite group of order n and let m be an integer that is relatively prime $|G|=n$. Then

(a) for any $a\in G\ \exists$ a unique element $b\in G$ such that $b^n=a$

(b) for any $a\in G\exists$ a unique element $b\in G$ such that $b^m=a$

(c) for some $a\in G\ \exists$ a unique element $b\in G$ such that $b^m=a$

(d) for any $a\in G\not\exists$ any element $b\in G$ such that $b^m=a$

Soln. Since m, n relatively prime integers, $\exists$ integers s, t such that $sm+tn=1$

Then, we have for any $a\in G$

$$a=a^1=a^{sm+tn}=a^{sm}a^{tn} \qquad ...(i)$$

Since $|G|=n$

$$\Rightarrow a^{tn}=\left(a^n\right)^t=e^t=e$$

Putting $b=a^s$, we have from (i) that $a=b^m e=b^m$

Now we show uniqueness of such b. suppose there is another $g'\in G$ such that

$a = (g')^m$

$b^m = a = (g')^m$

$b^{sm} = (g')^{sm}$

$b^{1-tn} = (g')^{1-tn}$

$b = g'$

Hence b is unique.

$\therefore$ option (b) is correct (a) , (c), (d) are false

Correct option is (b)

61. Let P be a prime number and G be a non abelian p-group, then

(a) the index of centre of G is divisible by p^2

(b) the index of centre of G need not be divisible by p^2

(c) the index of centre of G is only divisible by p

(d) None of these

Soln. Suppose the order of the group G is p^{α}, for some $\alpha \in Z$

Let $Z(G)$ be the centre of G. Since $Z(G)$ is subgroup of G the order of the centre is also a power of p i.e. $|Z(G)| = p^b$ for some $b \in \mathbb{Z}$

then we have the index $[G : Z(G)] = p^{a-b}$

If $a - b = 0$, then we have $G = Z(G)$ and G is an abelian group. This is contradictions with the assumption that G is non abelian. So, $a - b \neq 0$

If $a - b = 1$, then the order of $\left|\frac{G}{Z(G)}\right| = p$ is a prime, there $\frac{G}{Z(G)}$ is a cylic group

$\Rightarrow G$ is abelian which is contradiction

$\therefore$ we must have $a - b \geq 2$

hence p^2 divides the index [G: Z(G)] = p^{a-b}

option (a) is correct, (b) (c) are false.

62. Let G be a finite commutative group such that G contains two distinct element of order 2 Then

(a) |G| must be multiple of 4

(b) |G| must be multiple of 6

(c) If G is non commutative then |G| must be multiple of 4

(d) None of these

Soln. Let a, b, be two distinct element of order 2.

Let $H = \{e, a\}$ and $K = \{e, b\}$. Now H and K are subgroup of G. Since G is commutative

$HK = \{e, a, b, ab\}$ subgroup of order 4.

Now $|HK| = 4 | o(G)|$

Thus $|G|$is multiple of 4

$\therefore$ (a) is true and (b) is false

Take $G = S_3$ is non commutative, (12) and (13) are elements of S_3, and each is of order 2. But $4 \nmid |S_3| = 6$

Option (c) is false

Correct option is (a)

63. Let G be a finite non trivial group, then choose the correct statements

(a) If $\forall x \in G \; \exists \; y \in G$ such that $x = y^2$. Then the order of G is odd

(b) If $\forall x \in G \; \exists y \in G$ such that $x = y^2$. Then the order of G is even

(c) If |G| = odd then $\forall$x $\in$ G $\exists$ y $\in G$ that $x = y^2$.

(d) If |G| = even then $\forall x \in G \; \exists \; y \in G$ such that $x = y^2$.

Soln. Suppose G is of odd order i.e. $|G| = 2n+1$ for some positive integer and $\forall x \in G, x^{2n+1} = e$.

Now $x^{2n+1} = e \Rightarrow x = x^{-2n} = \left(x^{-n}\right)^2 = y^2$, where $y = x^{-n}$

$\therefore$ option (c) is true

Converse suppose |G| is not odd, let $|G|$ =$2n$ and $x \in G$ then $\exists \; y \in G$ such that $x = y^2$

$\therefore \; x^n = y^{2n} = e$

Then $\forall x \in G, x^n = e$ suppose n is odd say $n = 2m+1$. Then $x^{2m+1} = e \; \forall \; x \in G$.

$\exists \; z \in G$ such that $z \neq e$ and $z^2 = e$ (since |G| is even).

Hence $e = z^{2m+1} = zz^{2m} = z\left(z^2\right)^m$

$= ze = z,$ which is a contradiction. So n is even, say n = 2m then $x^{2m} = e \forall x \in G$ and we can show $x^m = e \; \forall x \in G$ and m is even continuing in this way, we can conclude that

$x^2 = e \; \forall x \in G$.

Let $x \in G$ then $\exists y \in G$ such that $x = y^2$, $\therefore$ x = e.

Thus $|G| = 1$ which is contradiction, consequently, G is of odd order

$\therefore$ option (a) is true and (d), (b) are false

Correct option are (a) and (c)

PRACTICE SET – 1

[Multiple Answer Type Questions]

1. Which is not a group.

(*a*) $(\mathbb{N}, +)$

(*b*) $(\mathbb{N}, *) : a * b = l.c.m.\,(a, b)$

(*c*) $(\mathbb{N}, +) : a * b = \min \cdot (a, b)$

(*d*) $(G,*), G=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix}\right\}: a, b, c, d \in \mathbb{Z}$ and $\begin{bmatrix} a & b\\ c & d\end{bmatrix} * \begin{bmatrix} a' & b'\\ c' & d'\end{bmatrix} = \begin{bmatrix} aa' & bb'\\ cc' & dd'\end{bmatrix}$

2. Which is not a group.

(*a*) $(\mathbb{N}, *), a * b = H.C.F.(a, b)$

(*b*) $(G,*), \left\{\begin{bmatrix} x & y\\ -\bar{y} & \bar{x}\end{bmatrix}: x, y \in \right\} * \to o.m.m.$ (ordinary matrix multiplication)

(*c*) $a, b \in \mathbb{N}$

$a * b = c$ where *c* is atleast 1 less than *a* + *b*. $(\mathbb{N}, *)$

(*d*) $(\mathbb{N}, *): a, b \in \mathbb{N}$,

$a * b = c$ where *c* is atmost one less than *a* + *b*.

3. Which of the following statement is/are true?

(*a*) Every element except identity can have order 4 in a group.

(*b*) Every element except identity can have order 7 in a group.

(*c*) Number of elements of order 2 can not be 6 in any group.

(*d*) None of these.

4. In an abelian group, the order of an element *a* is 4 and the order of an element *b* is 3 then $(ab)^4$ is

(*a*) a^2b^{-1} (*b*) $(ab)^{-2}$ (*c*) a^2 (*d*) *b*

5. If *G* is a group of order 10 then

(*a*) It must have a subgroup of order 5.

(*b*) It may have a subgroup of order 2.

(*c*) It must have exactly two subgroup of order 5.

(*d*) None of the above.

6. Let $H = \{x \in U(20) : x \equiv 1 (\text{mod } 3)\}$ then *H*

(*a*) Is a subgroup of $U(20)$.

(*b*) Is not a subgroup as not closed.

(*c*) Is not a subgroup as same elements have no inverse.

(*d*) Has no identity element.

[Single Correct Answer Type Questions]

7. Let *G* be a finite group with more than one element then *G* has an non-identity element of

(*a*) Prime order (*b*) Composite order (*c*) Order 2 (*d*) Odd order

8. Consider the following statement

(*i*) Let $H = \{a + b : a, b \in \mathbb{R}, a\, b \geq 0\}$ then *H* is a subgroup of $\mathbb{C} - \{0\}$ under multiplication.

(*ii*) Let there exists a group which has elements of every finite order and also of infinite order. Now choose the correct answer.

(*a*) 1 is correct and 2 is incorrect. (*b*) 2 is correct 1 is incorrect.

(*c*) Both 1 and 2 are correct. (*d*) Both 1 and 2 are incorrect.

9. Let *G* be a finite group of order-*n* which is not true :

(*a*) If *G* has a subgroup of order *m* then *m*|*n*.

(*b*) If G has an element of order m then $m|n$.

(*c*) If $m|n$, then G must have an element of order $m|n$.

(*d*) If $m|n$, m is prime, then G must have an element of order m.

10. Consider for $(Z \neq 0)$, $f_1(Z) = Z,\ f_2(Z) = -Z,\ f_3(Z) = \dfrac{1}{Z},\ f_4(Z) = \dfrac{-1}{Z}$ group $G = \{f_1, f_2, f_3, f_4\}$ under the operation of the composition of mapping the inverse of $f_1^{-1} \cdot f_2^{-1} \cdot f_3^{-1} \cdot f_4^{-1}$ is

(*a*) f_1 (*b*) f_2 (*c*) f_3 (*d*) f_4

11. If the orders of a and x in a group are respectively 3 and 4. Then the order of $x^{-1}a\ x$ is

(*a*) 3 (*b*) 4 (*c*) 6 (*d*) 12

12. Let G be a cyclic group of order 6. Then the number of elements $g \in G$ s.t. $G = \langle g \rangle$ is

(*a*) 5 (*b*) 3 (*c*) 4 (*d*) 2

13. Let I be the set of irrational real numbers and let $G = I \cup \{0\}$. Then, under the usual addition of real numbers. G is

(*a*) A group, since $\mathbb{R}$ and $\mathbb{Q}$ are groups under addition.

(*b*) A group, since the additive identity is in G.

(*c*) Not a group, since addition on G is not a binary operation.

(*d*) Not a group, since not all elements in G have an inverse.

14. Suppose G is a group with more than one element and no proper subgroup. Then the cardinality of G is
P : prime number ; Q : a finite non prime number ; R : infinite

(*a*) P only (*b*) P or Q, but not R

(*c*) P or R, but not Q (*d*) any of P, Q, R

[Numerical Answer Type Question]

15. Cardinality of the generators of $\mathbb{Z}_{30}$?

16. Find the cardinality of the group G if $a, b \in G$ such that $|a| = |b| = 2$ and $|ab| = 3$?

17. Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$. Then find the relation between $o(A)$ and $o(AB)$ where $A, B \in SL(2, \mathbb{R})$.

18. If a group of order 6 which is not abelian. Then how many subgroups does it have ?

19. Let $G = GL(2, \mathbb{R})$. Find $Z(G)$ = ?

20. Let G be a group $a \in G$ and $a \neq e$ s.t. $a^{20} = e$. Then if $o(G) = 10$. Then possible order of a if order of a is always odd ?

Solutions of Practice Set-1

[Multiple Answer Type Questions]

1. (*a*) $(\mathbb{N}, +)$ since it does not have identity.

(*b*) $(\mathbb{N}, *)$; $a * b = \text{l.c.m.}\,(a, b)$ inverse does not exist

(*c*) $(\mathbb{N}, +)$; $a * b = \min\,(a, b)$ identity not exist.

(*d*) $(G,*)$ inverse does not exist of each elements.

Ans. $(a), (b), (c)$ and (d)

2. $(a), (c), (d)$

3. $(b), (c)$ for any prime *p*. Group of order *p* has $p-1$ elements of order *p*. And also any group always has odd number of elements of order 2.

4. (*d*) since group is abelian,

so $(ab)^4 = a^4 \cdot b^4$ and $o(a)=4,\ o(b)=3$

so $a^4 = e$ also $b^4 = (b^3)\cdot b = e\cdot b = b$

$\Rightarrow (ab)^4 = e\cdot b = b$

5. (*a*), (*b*)

6. $H=\{1, 7, 13, 19\}$

(*b*) since $13 \times_{20} 7 = 11 \notin H$

(*c*) $7^{-1} = 3 \notin H$

so answer are (*b*) and (*c*)

[Single Correct Answer Type Questions]

7. (*a*) prime order

8. (*b*) since *H* contains '0' also which is not in $\mathbb{C}-\{0\}$. Hence *H* can not be subgroup of $\mathbb{C}-\{0\}$. Also $(\mathbb{C}-\{0\},\times)$ is a group which have properties described in statement (*ii*)

9. (*c*) A_4 alternative group $o(A_4)=\dfrac{4!}{2}$ also $6\left|\left(\dfrac{4!}{2}\right)\right.$ but there is no subgroup of order 6.

10. (*a*) f_1

11. (*a*)

$o(a)=3,\quad o(x)=4,\quad o(x^{-1}a\,x)=?$

$(x^{-1}a\,x)^3 = a^3\,e \Rightarrow x^{-1}a^3x = e\ \Rightarrow x^{-1}a^3x = e \Rightarrow x^{-1}e\cdot x = e$

12. (*d*) since $\phi(6)=2=$ number of generators.

13. (*c*) since it fails closure property.

14. (*a*)

[Numerical Answer Type Questions]

15. $\phi(30)=\phi(2)\cdot\phi(3)\cdot\phi(5)=(1)\,(2)\cdot 4 = 8$

16. 6

17. $o(A) < o(AB)$ since $o(A)$ is finite but $o(AB)$ is infinite

18. 6

19. $G = G\,L\,(2,\mathbb{R})$. To find $Z(G)=$??

$Z(G)=$ All scalar matrices in $G\,L\,(2,\mathbb{R})$

Chapter 3

CYCLIC GROUPS

Order of an Element: The order of an element 'g' in a group G is the smallest positive integer 'n' such that $g^n = e$. (In additive notation, this would be $ng = 0$, i.e. it depend on group operation) If no such integer exists, we say 'g' has infinite order. The order of an element 'g' is denoted by $|g|$ or 'o'(g).

Example - 1: Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. To find the order of 7 we compute the sequence $7^1 = 7$, $7^2 = 4$, $7^3 = 13$, $7^4 = 1$, so $|7| = 4$. To find the order of 11, we compute $11^1 = 11$, $11^2 = 1$, so $|11| = 2$. Similar computations show that $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$, $|4| = 2$. [Here is a trick that makes these calculations easier. Rather than compute the sequence 13^1, 13^2, 13^3, 13^4, we may observe that $13 = -2$ modulo 15 (since $13 + 2 = 0$ mod 15) so that $13^2 = (-2)^2 = 4$, $13^3 = -2.4 = -8$, $13^4 = (-2)(-8) = 1$].

Example - 2: Consider $\mathbb{Z}_{10}$ under addition modulo 10. Since $1.2 = 2$, $2.2 = 4$, $3.2 = 6$, $4.2 = 8$, $5.2 = 0$ $\Rightarrow |2| = 5$. Similar computations show that $|0| = 1$, $|7| = 10$, $|5| = 2$, $|6| = 5$.

Example - 3: Consider $\mathbb{Z}$ under ordinary addition. Here every non-zero element has infinite order, since the sequence a, $2a$, $3a$, ... never includes 0 when $a \neq 0$.

Cyclic Groups: Definition: A group G is called cyclic if, for some $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. The element a is called a generator of G.

Examples:

(i) The set of integers $\mathbb{Z}$ under addition is cyclic, both 1 and –1 are generators.

$1^n = n = \underbrace{1+1+......1}_{n\text{ times}}$ when n is positive and $-n = \underbrace{(-1)+(-1)+.......+(-1)}_{|n|\ times}$ when n is negative.

(ii) The set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n.

Here 1 and $-1 (= n - 1)$ are again generators.

Unlike $\mathbb{Z}$, which has only two generators, $\mathbb{Z}_n$ may have many generators (depending on which n we are given).

(iii) $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = <3>$

Also $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = <7>$

So both 3 and 7 are generators for $U(10)$.

Theorem: Order of a cyclic group is equal to the order of its generator.

Proof: Let $G = < a >$ i.e., G is a cyclic group generated by a.

Case (i) : $o(a)$ is finite, say n, then n is the least positive integer such that, $a^n = e$.

Consider the elements $a^0 = e, a, a^2, ..., a^{n-1}$; these are all elements of G and are n in number.

Suppose any two of the above elements are equal say $a^i = a^j$ with $i > j$ then $a^i.a^{-j} = e \Rightarrow a^{i-j} = e$

But $0 < i - j \leq n - 1 < n$, thus $\exists$ a positive integer $i - j$, s.t. $a^{i-j} = e$ and $i - j < n$, which is a contradiction to the fact that $o(a) = n$.

Thus no two of the above n elements can be equal i.e., G contains at least n elements. Now, we show that it does not contain any other element. Let $x \in G$ be any element. Since G is cyclic, generated by a, x will be some power of a.

Let $\quad x = a^m$

By division algorithm, we can write $m = nq + r$ where $0 \le r < n$

Now $\quad a^m = a^{nq+r} = (a^n)^q . a^r = e^q . a^r = a^r$

$\Rightarrow x = a^r$ where $0 \le r < n$

i.e., x is one of $a^0 = e, a, a^2, ..., a^{n-1}$ or G contains precisely n elements

$\Rightarrow o(G) = n = o(a)$

Case (ii): $o(a)$ is infinite

In this case no two powers of a can be equal as if $a^n = a^m (n > m)$ then $a^{n-m} = e$, i.e., it is possible to find a positive integer $n - m$ such that, $a^{n-m} = e$ meaning thereby that a has finite order.

Hence no two powers of a can be equal. In other words G would contain infinite number of elements.

Problem: If $a \in G$ be of finite order n and also $a^m = e$ then show that $n|m$.

Soln: Let $o(a) = n$, then by definition n is the least positive integer such that $a^n = e$.

Suppose $a^m = e$ for some m. By division algorithm $m = nq + r$ where $0 \le r < n$.

$\Rightarrow e = a^m = a^{nq} . a^r = (a^n)^q . a^r = e^q . a^r = a^r$ where $0 \le r < n$

Since n is such least positive integer, we must have $r = 0$

i.e., $m = nq$ or $n | m$.

Theorem: (Criterion for $a^i = a^j$): Let G be a group, and let a belongs to G. If a has infinite order, then all distinct powers of a are distinct group elements, If a has finite order, say, n, then $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Corollary: ($a^k = e$ implies that $|a|$ divides k):

Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

Proof: Since $a^k = e = a^0$, we know by above theorem that n divides $k - 0 \Rightarrow n | k$

Theorem: The order of every element of a finite group is finite and is less than or equal to the order of the group..

Theorem: The order of an element of a group is the same as that of its inverse a^{-1}.

Proof: Let n and m be the orders of a and a^{-1} respectively.

We have $o(a) = n \Rightarrow a^n = e$ (identity element)

$$\Rightarrow (a^n)^{-1} = e^{-1} \Rightarrow (a^{-1})^n = e \Rightarrow o(a^{-1}) \le n \Rightarrow m \le n$$

Also $o(a^{-1}) = m \Rightarrow (a^{-1})^m = e \Rightarrow (a^m)^{-1} = e \Rightarrow a^m = e \; [\because b^{-1} = e \Rightarrow b = e]$

$$\Rightarrow o(a) \le m \Rightarrow n \le m$$

Now $m \le n$ and $n \le m \Rightarrow m = n$

If the order of a is infinite, then the order of a^{-1} cannot be finite.

Because, $o(a^{-1}) = m \Rightarrow o(a) \le m \Rightarrow o(a)$ is finite. Therefore if the order a is infinite, then the order of a^{-1} must be infinite.

Theorem: The orders of the elements a and $x^{-1}ax$ are the same where a, x are any two elements of a group.

Corollary: Order of ab is the same as that of ba where a and b are any elements of a group.

Proof: We have $a^{-1}(ab)a = (a^{-1}a)(ba) = e(ba) = ba$

Thus, $ba = a^{-1}(ab)a$

$\Rightarrow$ Order of ba = order of $a^{-1}(ab)a$

$\Rightarrow$ Order of ba = order of ab $[\because o(x^{-1}ax) = o(a)]$

Theorem: If 'a' is an element of order n and p is prime to n, then a^p is also of order n.

Proof: Let m be the order of a^p.

Now, $o(a) = n \Rightarrow a^n = e \Rightarrow (a^n)^p = e^p = e$

$\Rightarrow (a^p)^n = e \Rightarrow o(a^p) \le n \Rightarrow m \le n$

Since p, n are relative primes, there exist integers x and y such that $px + ny = 1$

$\therefore a = a^1 = a^{px+ny} = a^{px}\, a^{ny} = a^{px}(a^n)^y = a^{px}e^y = a^{px}e = a^{px} = (a^p)^x$

Now, $a^m = [(a^p)^x]^m = (a^p)^{mx} = [(a^p)^m]^x$

$= e^x$ $[\because o(a^p) = m \Rightarrow (a^p)^m = e] = e$

$\therefore o(a) \le m \Rightarrow n \le m$

Finally, $m \le n$ and $n \le m$ $\Rightarrow m = n$

Ex.1: Prove that if $a^2 = a, a \in G$, then $a = e$.

Soln. We have, $a^2 = a \Rightarrow aa = a \Rightarrow aa = ae$ $[\because ae = a]$

$\Rightarrow a = e$ [by left cancellation law in G]

Ex. 2: Given $axa = b$ in G, find x.

Soln. We have, $axa = b \Rightarrow a^{-1}(axa) = a^{-1}b$

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

$\Rightarrow (xa)a^{-1} = a^{-1}ba^{-1} \Rightarrow x(aa^{-1}) = a^{-1}ba^{-1} \Rightarrow xe = a^{-1}ba^{-1}$

$\Rightarrow x = a^{-1}ba^{-1}$

Ex. 3: If a and b are any elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$ for any integer n.

Soln. (i) For n = 0. We have,.

$(bab^{-1})^0 = e$ [by definition]

Also, $ba^0b^{-1} = beb^{-1} = bb^{-1} = e$

$\therefore (bab^{-1})^0 = ba^0b^{-1}$

(ii) For $n > 0$. We have, $(bab^{-1})^1 = bab^{-1} = ba^1b^{-1}$ $[\because a^1 = a]$

Thus the result is true for n = 1.

Let us suppose that the result is true for $n = k$ i.e., suppose $(ba\ b^{-1})^k = ba^k b^{-1}$

Then $(ba\ b^{-1})^{k+1} = (ba\ b^{-1})^k (ba\,b^{-1})^1 = ba^k b^{-1} ba\,b^{-1}$

$= ba^k\ eab^{-1} = ba^k\ ab^{-1} = ba^{k+1} b^{-1}$

Therefore, the result is true for $n = k+1$ if it was true for $n = k$. But we have seen that the result is true for $n = 1$. Hence by mathematical induction it is true for all $n > 0$.

(iii) For $n < 0$. Let $n = -m$ where $m > 0$.

Then $(ba\,b^{-1})^n = (ba\,b^{-1})^{-m} = [(ba\,b^{-1})^m]^{-1} = (ba^m\,b^{-1})^{-1}$

$= (b^{-1})^{-1}(a^m)^{-1} b^{-1} = ba^{-m} b^{-1} = ba^n b^{-1}$

Ex.4: Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(ab)^n = a^n b^n$.

Soln. (i) For $n = 0$. We have $(ab)^0 = e$

Also $a^0 b^0 = ee = e$

$\therefore \quad (ab)^0 = a^0 b^0$.

(ii) For $n > 0$. If $n = 1$, then $(ab)^1 = ab = a^1 b^1$.

Now suppose for $n = k$, $(ab)^k = a^k b^k$

Then $(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = a^k ab^k b$ $[\because G$ is abelian $\Rightarrow b^k a = ab^k]$

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

Thus the result is true for $n = k+1$ if it was true for $n = k$. But it is true for $n = 1$. Hence by mathematical induction for all $n > 0, (ab)^n = a^n b^n$.

(iii) For $n < 0$. Let $n = -m$ where m is a positive integer.

Then $(ab)^n = (ab)^{-m} = [(ab)^m]^{-1} = (a^m b^m)^{-1}$

$= (b^m a^m)^{-1}$ $[\because$ G is abelian $\Rightarrow a^m b^m = b^m a^m]$

$= (a^m)^{-1}(b^m)^{-1}$ $[\because (ab)^{-1} = b^{-1} a^{-1}]$

$= a^{-m} b^{-m} = a^n b^n$

Ex.5: Prove that if for every element a in a group G, $a^2 = e$, then G is an abelian group.

Soln. Let a and b be any two elements of the group G. Then ab is also an element of G. Therefore $(ab)^2 = e$.

Now $(ab)^2 = e \Rightarrow (ab)(ab) = e \Rightarrow (ab)^{-1} = ab$

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

But $a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$

Similarly, $b^2 = e \Rightarrow b^{-1} = b$

Therefore, from (1), we get $ba = ab$. Thus we have $ab = ba\ \forall a, b \in G$. Therefore G is an abelian group.

Ex.6: Prove that a group G is abelian if every element of G except the identity element is of order two.

Soln. Identity element e is of order 1. But $e^2 = e$. Since every other element is of order two, therefore we have $a^2 = e\ \forall a \in G$.

Now proceed as in Ex. 5.

Ex.7: Show that if every element of a group *G* is its own inverse, then *G* is abelian.

Soln. Let *a* and *b* be any two elements of *G*. Then *ab* is also an element of *G*. Therefore $(ab)^{-1} = ab$ as it is given that every element is its own inverse.

Now $(ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab \;\; \Rightarrow ba = ab \;\; [\because a^{-1} = a, b^{-1} = b]$

Thus, we have $ab = ba \, \forall a, b \in G$. Therefore *G* is an abelian group.

Ex.8: Show that if *a*, *b* are any two elements of a group *G*, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Soln. Suppose *G* is abelian.

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

$= a(ab)b \;\; [\because G$ is abelian $\Rightarrow ab = ba]$

$= (aa)(bb) = a^2b^2$

Conversely, let a, b be any two elements of *G*.

Then $(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)(bb) \Rightarrow a(ba)b = a(ab)b$

$\Rightarrow (ba)b = (ab)b$ [by left cancellation law]

$\Rightarrow ba = ab$ [by right cancellation law] $\Rightarrow G$ is abelian.

Ex.9: Prove that a group *G* is abelian if $b^{-1}a^{-1}ba = e, \forall a, b \in G$.

Soln. We have $b^{-1}a^{-1}ba = e \Rightarrow (b^{-1}a^{-1})(ba) = e$

$\Rightarrow (b^{-1}a^{-1})^{-1} = ba \;\; [\because ab = e \Rightarrow a^{-1} = b]$

$\Rightarrow (a^{-1})^{-1}(b^{-1})^{-1} = ba \;\; [\because (ab)^{-1} = b^{-1}a^{-1}]$

$\Rightarrow ab = ba \;\; [\because (a^{-1})^{-1} = a]$

$\Rightarrow G$ is abelian.

Ex.10: If *G* is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.

Soln. Let *G* be a group of even order 2*n*, where *n* is a positive integer. We shall prove that *G* must have an element $a \neq e$ such that $a^{-1} = a$. We shall prove it by contradiction.

Suppose *G* has no element, other than the identity element *e*, which is its own inverse. Now in a group every element possesses a unique inverse. The identity element *e* is its own inverse. Further if *b* is the inverse of *c*, then *c* is the inverse of *b*. So excluding the identity element *e*, the remaining $2n-1$ elements of *G* must be divided into pairs of two such that each pair consists of an element and its inverse. But we cannot do so because the odd integer 2*n*–1 is not divisible by 2. Hence our initial assumption is wrong.

So in *G* there is an element $a \neq e$ such that $a = a^{-1} \Rightarrow aa = a^{-1}a \Rightarrow a^2 = e$

Ex.11: If a group *G* has four elements, show that it must be abelian.

Soln. Let $G = \{e, a, b, c\}$ be a group of order four. Here *e* is the identity element. The identity element *e* is its own inverse. There must be at least one more element in *G* which is its own inverse.

Let $a^{-1} = a$. If $b^{-1} = b$ and $c^{-1} = c$, then definitely *G* is abelian.

If $b^{-1} = c$, then $c^{-1} = b$ and we have $bc = e = cb$. Also $a^{-1} = a \Rightarrow aa = e$.

In this case the composition table for *G* will be as follows:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Note that ab would have been either equal to b or equal to c. Since $ab=b \Rightarrow a=e$, therefore ab must be equal to c. Then ac will be equal to b.

Now we can easily complete the table since in each column each element must be distinct and in each row each element must be distinct. From the table we see that composition in G is commutative. Therefore G is abelian.

Ex.12: If G is a group such that $(ab)^m=a^mb^m$ for three consecutive integers m and for all $a,b\in G$, show that G is abelian.

Soln. Let a,b be any two elements of G. Suppose m, $m+1, m+2$ are three consecutive integers such that $(ab)^m=a^mb^m$, $(ab)^{m+1}=a^{m+1}b^{m+1}$ and $(ab)^{m+2}=a^{m+2}b^{m+2}$.

We have,

$(ab)^{m+2}=(ab)^{m+1}(ab)$

$\Rightarrow a^{m+2}\,b^{m+2}=a^{m+1}b^{m+1}(ab)$ (Given)

$\Rightarrow aa^{m+1}\,b^{m+1}\,b=a\;a^m\;b^m\;bab$

$\Rightarrow a^{m+1}\,b^{m+1}=a^mb^mba$ [by left and right cancellation laws]

$\Rightarrow (ab)^{m+1}=(ab)^m ba \Rightarrow (ab)^m(ab)=(ab)^m(ba)\Rightarrow ab=ba$ [by left cancellation law]

$\Rightarrow G$ is abelian.

Ex.13: In a group, if $ba=a^mb^n$, prove that the elements $a^mb^{n-2}, a^{m-2}b^n, ab^{-1}$ have the same order.

Soln. We have,

$a^mb^{n-2}=a^mb^nb^{-2}=bab^{-2}$ [$\because ba=a^mb^n$]

$=ba\;b^{-1}\,b^{-1}=(b^{-1})^{-1}(ab^{-1})b^{-1}$

Now, we know that in a group $o(a)=o(x^{-1}ax)$, where a, x are any two elements of the group.

$\therefore o(a^m\,b^{n-2})=o[(b^{-1})^{-1}(ab^{-1})b^{-1}]=o(ab^{-1})$ ...(1)

Further $a^{m-2}b^n=a^{-2}a^mb^n=a^{-2}ba=a^{-2}ba^{2-1}=a^{-2}ba^{-1}a^2$

$=(a^2)^{-1}(ba^{-1})a^2$

$\therefore o(a^{m-2}\,b^n)=o[(a^2)^{-1}(ba^{-1})a^2]=o(ba^{-1})$

$=o[(ba^{-1})^{-1}]$, since $o(a^{-1})=o(a)$

$=o[(a^{-1})^{-1}b^{-1}]=o(ab^{-1})$ ... (2)

From (1) and (2), we get $o(a^mb^{n-2})=o(ab^{-1})=o(a^{m-2}b^n)$

Ex.14: If in the group G, $a^5 = e, aba^{-1} = b^2$ for $a, b \in G$, find $o(b)$.

Soln. We have,

$$(ab\,a^{-1})^2 = ab\,a^{-1}ab\,a^{-1} = ab^2a^{-1} = aa\,ba^{-1}a^{-1} \quad [\because ab\ a^{-1} = b^2]$$

$$= a^2\,ba^{-2}$$

$$\therefore (ab\,a^{-1})^4 = \{(ab\,a^{-1})^2\}^2 = (a^2ba^{-2})^2 = a^2ba^{-2}a^2ba^{-2}$$

$$= a^2b^2a^{-2} = a^2ab\,a^{-1}a^{-2} = a^3ba^{-3}$$

$$\therefore (a\,ba^{-1})^8 = \{(ab\,a^{-1})^4\}^2 = (a^3ba^{-3})^2 = a^3ba^{-3}a^3ba^{-3} = a^3b^2a^{-3}$$

$$= a^3ab\,a^{-1}a^{-3} = a^4\,ba^{-4}$$

$$\therefore (aba^{-1})^{16} = \{(ab\,a^{-1})^8\}^2 = (a^4\,ba^{-4})^2 = a^4ba^{-4}a^4ba^{-4} = a^4b^2a^{-4}$$

$$= a^4a\,ba^{-1}a^{-4} = a^5\,ba^{-5}$$

$$= ebe \ [\because a^5 = e \text{ and so } a^{-5} = e]$$

$= b$

Thus, $(aba^{-1})^{16} = b$

$\therefore (b^2)^{16} = b$ $\qquad\qquad [\because ab\,a^{-1} = b^2]$

$\Rightarrow b^{32} = b \Rightarrow b^{31} = e$

Since $b^m = e \Rightarrow o(b) \mid m$, therefore $o(b) \mid 31$

But 31 is a prime integer. Therefore $o(b) = 1$ or 31.

So if $b = e$, then $o(b) = 1$ and $b \neq e$ then $o(b) = 31$.

Ex.15: If *G* is a finite abelian group with elements $a_1, a_2, ..., a_n$, prove that $a_1a_2...a_n$ is an element whose square is the identity.

Soln. We have $(a_1a_2...a_n)^2 = (a_1a_2...a_n)(a_1a_2...a_n)$ ... (1)

Now each element in a group has a unique inverse. Therefore each of $a_1, a_2, ..., a_n$ is the inverse of exactly one of them. So associating each of $a_1, a_2, ..., a_n$ with its inverse, the relation (1) becomes

$(a_1a_2...a_n)^2 = (a_1a_1^{-1})(a_2a_2^{-1})....(a_na_n^{-1}) = eee.....$ upto *n* times = *e*. [since, group is abelian].

Ex.16: Show that the equation $x^2ax = a^{-1}$ is solvable for *x* in a group *G* if and only if *a* is the cube of some element in *G*.

Soln. Suppose $x^2ax = a^{-1}$ is solvable in *G*. Then there exists an element $c \in G$ such that $c^2ac = a^{-1}$.

Now $c^2ac = a^{-1} \Rightarrow ccac = a^{-1}$

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

$= e \Rightarrow (ca)(ca) = c^{-1} \Rightarrow (ca)(ca)c = c^{-1}c \Rightarrow (ca)(ca)c = e$

$\Rightarrow (ca)\ (ca)ca = a \Rightarrow (ca)^3 = a \Rightarrow a$ is the cube of some element $ca \in G$.

Conversely, let $a = b^3$ for some $b \in G$. Then $x = b^{-2}$ is a solution of $x^2ax = a^{-1}$. For if $x = b^{-2}$ and $a = b^3$, then $x^2ax = b^{-4}b^3b^{-2} = b^{-3} = (b^3)^{-1} = a^{-1}$. Thus $x = b^{-2}$ is a solution of $x^2ax = a^{-1}$.

Ex.17: If in a group *G*, $xy^2 = y^3x$ and $yx^2 = x^3y$, then show that $x = y = e$ where *e* is the identity of *G*.

Soln. We have,

$$xy^2 = y^3x \Rightarrow x^2y^2 = xy^3x$$

$$\Rightarrow x^2y = xy^3xy^{-1} = xy^2yxy^{-1} = y^3xyxy^{-1} \qquad ...(1)$$

Again, $yx^2 = x^3y \Rightarrow yx^2 = xx^2y$

$\Rightarrow yx^2 = xy^3xyxy^{-1}$, substituting for x^2y from (1)

$$\Rightarrow x^2 = y^{-1}xy^3xyxy^{-1}$$

$$\Rightarrow x^2y = y^{-1}xy^3xyx \qquad ...(2)$$

From (1) and (2), we get $y^3xyxy^{-1} = y^{-1}xy^3xyx$

$$\Rightarrow y^4xyx = xy^3xyxy = xy^2yxyxy = y^3xyxyxy$$

Cancelling y^3 from both sides, we get $yxyx = xyxyxy$

$$\Rightarrow (yx)^2 = (xy)^3 \qquad ...(3)$$

Since the given relations are symmetrical in *x* and *y*, therefore interchanging *x* and *y* in (3), we get

$$(xy)^2 = (yx)^3 \qquad ...(4)$$

Now from (3) and (4), we have

$$(xy)^2 = (yx)^3 = (yx)^2(yx) = (xy)^3(yx)$$

Cancelling $(xy)^2$ from both sides, we get $e = (xy)(yx) = xy^2x \Rightarrow x^{-2} = y^2$

Now $xy^2 = y^3x \Rightarrow xx^{-2} = yx^{-2}x \Rightarrow x^{-1} = yx^{-1} \Rightarrow y = e$

Again $yx^2 = x^3y \Rightarrow ex^2 = x^3e \Rightarrow x^2 = x^3 \Rightarrow x = e$

Ex.18: Let *G* be a group and let $a \in G$ be of finite order *n*. Then for any integer *k*, we have $o(a^k) = \dfrac{n}{(n,k)}$ where (*n*, *k*) denotes the gcd of *n* and *k*.

Soln. Let $(n,k) = m$. Then we have *n* = *pm*, *k* = *qm* for some integers *p* and *q* such that (*p*, *q*) = 1.

Let $o(a^k) = l$.

$$(a^k)^l = e \Rightarrow a^{kl} = e$$

$\Rightarrow n \mid kl$ $\qquad$ $[\because o(a) = n; \therefore a^{kl} = e \Rightarrow n \mid kl]$

$$\Rightarrow pm \mid qml \Rightarrow p \mid ql$$

$\Rightarrow p \mid l$ $\qquad$ [$\because$ *p* and *q* are relatively prime]

Again, $(a^k)^p = (a^{qm})^p = a^{qmp} = a^{qn} = (a^n)^q = e^q = e$

Therefore, $o(a^k) \mid p$ i.e. $l \mid p$

Now, $l \mid p$ and $p \mid l \Rightarrow l = p$

$$\therefore o(a^k) = p = \frac{n}{m} = \frac{n}{(n,k)}$$

(a) Problem: If *G* is a finite abelian group then show that $o(ab)$ is a divisor of 1.c.m. of $o(a), o(b)$.

Soln. Let $o(a) = n, o(b) = m, o(ab) = k$

Let $l = l.c.m.(m,n)$ then $m\,|\,l, n\,|\,l, \Rightarrow l = mr_1, l = nr_2$

Now $(ab)^l = a^l b^l$ (G is abelian)

$= a^{nr_2} b^{mr_1} = e.e = e \Rightarrow o(ab)\,|\,l \Rightarrow k\,|\,l$

Some properties of cyclic groups:

Theorem: Every cyclic group is an abelian group, but not conversely.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by *a*. Let *x*, *y* be any two elements of *G*. Then there exist integers *r* and *s* such that $x = a^r, y = a^s$. Now $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s\, a^r = yx$. Thus we have $xy = yx \,\forall\, x, y \in G$. Therefore *G* is abelian.

Theorem: If *a* is a generator of a cyclic group *G*, then a^{-1} is also a generator of *G*.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by *a*. Let a^r be any element of *G*, where *r* is some integer. We can write $a^r = (a^{-1})^{-r}$. Since –*r* is also some integer, therefore each element of *G*, is generated by a^{-1}. Thus a^{-1} is also a generator of *G*.

Example (*i*) In $\mathbb{Z}_{10}$; one generator is 1 then its inverse will also be the generator of $\mathbb{Z}_{10}$. And in $\mathbb{Z}_{10}$, $(1)^{-1} = 10 - 1 = 9$. Hence 9 is also a generator of 1.

Theorem: If a finite group of order *n* contains an element of order *n*, the group must be cyclic.

Proof. Suppose *G* is a finite group of order *n*. Let $a \in G$ and let *n* be the order of *a*. If *H* is the cyclic subgroup of *G* generated by *a* i.e., if $H = \{a^r : r \in I\}$, then the order of *H* is *n* because the order of the generator *a* of *H* is *n*. Thus *H* is a cyclic subgroup of *G* and the order of *H* is equal to the order of *G*. Hence *H* = *G* and therefore *G* itself is a cyclic group and *a* is a generator of *G*.

Example :

Theorem: Every cyclic group is an abelian group. But converse need not be true.

As K_4 : klein-4 group is abelian but not cyclic.

Since, order of K_4 is 4 but there is no element of order 4 in K_4. So, by the definition of cyclic group K_4 is not cyclic.

Example (*ii*) In $\mathbb{Z}$, 1 and –1 both are generator of $\mathbb{Z}$ and 1 and –1 are also inverse of each other.

In $\mathbb{Z}_2$, only 1 is generator, since 1 is inverse itself so, no other element of $\mathbb{Z}_2$ is generator except 1.

Generators of Cyclic Groups:

Theorem. Let $G = \langle a \rangle$ be a cyclic group of order *n*. Then $G = \langle a^k \rangle$ if and only if $\gcd(k,n) = 1$.

Proof. If $\gcd(k,n) = 1$, we may write $1 = ku + nv$ for some integers *u* and *v*. Then $a = a^{ku+nv} = a^{ku}.a^{nv} = a^{ku}$. Thus, *a* belongs to $\langle a^k \rangle$ and therefore all powers of *a* belongs to $\langle a^k \rangle$. So, $G = \langle a^k \rangle$ and a^k is a generator of *G*.

Now suppose that $\gcd(k,n) = d > 1$. $\Rightarrow$ $k = td$ and $n = sd$ for some integer *t* and *s*.

Then $(a^k)^s = (a^{td})^s = (a^{sd})^t = (a^n)^t = e,$ so that $|a^k| \le s < n$. This shows that a^k is not a generator of *G*.

Taking $G = \mathbb{Z}_n$ and *a* = 1 in theorem, we have the following useful result. [In particular, note that the generators of $\mathbb{Z}_n$ are precisely the elements of *U*(*n*)].

Corollary - Generators of $\mathbb{Z}_n$: An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k, n) = 1$.

The value of theorem is that once one generator of a cyclic group has been found, all generators of the cyclic group can easily be determined. For example, consider the subgroup of all rotations in D_6. Clearly one generator is R_{60}. And, since $|R_{60}| = 6$, we see by theorem that the only other generator is $(R_{60})^5 = R_{300}$. Of course, we could have readily deduced this information without the aid of theorem by direct calculations. So, to illustrate the real power of theorem, let us use it to find all generators of the cyclic group $U(50)$. First, note that direct computations show that $|U(50)| = 20$ and that 3 is one of its generators. Thus, in view of theorem, the complete list of generators for $U(50)$ is

$3 \bmod 50 = 3,\qquad 3^{11} \bmod 50 = 47,$
$3^3 \bmod 50 = 27,\qquad 3^{13} \bmod 50 = 23,$
$3^7 \bmod 50 = 37,\qquad 3^{17} \bmod 50 = 13,$
$3^9 \bmod 50 = 33,\qquad 3^{19} \bmod 50 = 17.$

Admittedly, we had to do some arithmetic here, but it certainly entailed much less work than finding all the generators by simply determining the order of each element of $U(50)$ one by one.

Theorem: Fundamental Theorem of Cyclic Groups: Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k-namely, $\langle a^{n/k}\rangle$.

Let's see what it means. Suppose $G = \langle a\rangle$ and G has order 30. The first part of the theorem says that if H is any subgroup of G, then H has the form $\langle a^k\rangle$ for some k. The second part of the theorem says that G has exactly one sub-group of each of the orders 1, 2, 3, 5, 6, 10, 15 and 30 and no others.

Corollary : Subgroups of $\mathbb{Z}_n$: For each positive divisor k of n, the set $\langle n/k\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Example: The list of subgroups of $\mathbb{Z}_{30}$ is

$\langle 1\rangle = \{0,1,2,\ldots,29\}$	order 30,
$\langle 2\rangle = \{0,2,4,\ldots,28\}$	order 15,
$\langle 3\rangle = \{0,3,6,\ldots,27\}$	order 10,
$\langle 5\rangle = \{0,5,10,15,20,25\}$	order 6,
$\langle 6\rangle = \{0,6,12,18,24\}$	order 5,
$\langle 10\rangle = \{0,10,20\}$	order 3,
$\langle 15\rangle = \{0,15\}$	order 2,
$\langle 30\rangle = \{0\}$	order 1.

By combining above two theorem, we can easily count the number of elements of each order in a finite cyclic group. For convenience, we introduce an important number-theoretic function called the *Euler phi function*. Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n. Notice that $|U(n)| = \phi(n)$.

Note: The following two results can be helpful at times:

(i) If $p_1, p_2, ..., p_k$ are distinct prime factors of $n(>1)$, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)....\left(1-\frac{1}{p_k}\right)$$

(ii) If *m*, *n* are co-prime then $\phi(mn) = \phi(m)\phi(n), (m, n \geq 1)$

Theorem: Number of Elements of each order in a Cyclic Group:

If *d* is a positive divisor of *n*, the number of elements of order *d* in a cyclic group of order *n* is $\phi(d)$.

Proof : By theorem, there is exactly one subgroup of order *d*-call it $\langle a \rangle$. Then every element of order *d* also generates the subgroup $\langle a \rangle$ and, by theorem, an element a^k generates $\langle a \rangle$ if and only if $\gcd(k, d) = 1$. The number of such elements is precisely $\phi(d)$.

Theorem : A group of finite composite order has at least one non-trivial subgroup.

Proof : Let $o(G) = n = rs$ where $1 < r, s < n$

Since, $n > 1, \exists\ e \neq a \in G$. Consider a^r.

Case (i): $a^r = e$

then, $o(a) \leq r$, let $o(a) = k$

then, $1 < k \leq r < n$ ($k > 1$, as $a \neq e$)

Let $H = \{a, a^2, a^3, ..., a^k = e\}$

then, *H* is a non-empty finite subset of *G* and it is closed under multiplication, thus *H* is a subgroup of *G*. Since $o(H) = k < n$, we have proved the result.

Case (ii): $a^r \neq e$ then since $(a^r)^s = a^{rs} = a^n = a^{O(G)} = e$

$o(a^r) \leq s$. Let $o(a^r) = t$ then $1 < t \leq s < n$.

If we take $K = \{a^r, a^{2r}, ..., a^{tr} = e\}$ then *K* is a non empty finite subset of *G*, closed under multiplication and is therefore a subgroup of *G*. Its order being less than *n*, it is required subgroup.

Theorem: If *G* is a group having no non-trivial subgroups then *G* must be finite having prime order.

Proof : Suppose *G* has infinite order.

Then, we can find $a \in G$, s.t., $a \neq e$.

Let $H = < a >$, then *H* is a cyclic subgroup of *G* and $H \neq \{e\}$. But *G* has no non-trivial subgroups.

Thus, $H = G \Rightarrow G = < a >$

Consider now the subgroup $K = <a^2>$

Now , $a \notin < a^2 >$, because if $a \in < a^2 >$ then $a = a^{2t}$ for some integer *t*

$\Rightarrow a^{2t-1} = e \Rightarrow o(a) \leq 2t - 1$

meaning thereby that $o(a)$ if finite, which is not true. Thus $a \notin < a^2 >$. Again $< a^2 > \neq \{e\}$, because then $a^2 = e$ would again mean that $o(a)$ is finite (≤ 2).

Thus $< a^2 >$ is a non-trivial subgroup of *G* which is not possible. Hence $o(G)$ cannot be infinite.

So $o(G)$ is finite and as it cannot be composite by previous theorem, it must be prime.

Summing up, what we have done above proves.

Theorem: An infinite cyclic group has precisely two generators.

Proof : Let $G = <a>$ be an infinite cyclic group.

As mentioned earlier, if a is a generator of G then so would be a^{-1}.

Let now b be any generator of G,

then as $b \in G$, a generates G, we get $b = a^n$ for some integer n. Again as $a \in G$, b generates G, we get $a = b^m$ for some integer m.

$\Rightarrow a = b^m = (a^n)^m = a^{nm}$

$\Rightarrow a^{nm-1} = e \Rightarrow o(a)$ is finite and $\leq nm - 1$

Since $o(G) = o(a)$ is infinite, the above can hold only if $nm - 1 = 0 \Rightarrow nm = 1$

$\Rightarrow m = \dfrac{1}{n}$ or $n = \pm 1$ as m, n are integers i.e., $b = a$ or a^{-1}

In other words, a and a^{-1} are precisely the generators of G.

Theorem: Number of generators of a finite cyclic group of order n is $\varphi(n)$.

Theorem: If a group has finite number of subgroups, then it is a finite group.

Theorem: The number of elements of prime order p in a finite group G is a multiple of p–1.

Solved Examples

1. Let G be a cyclic group such that G has an element of infinite order. Then the number of elements of finite order in G is. **[D U-2017]**

(a) 0 (b) 1 (c) infinite (d) none of these

Soln. Given G is a cyclic group and G has an element of infinite order

$\Rightarrow G$ is an infinite group

Also every infinite cyclic group is isomorphic to $(\mathbb{Z},+)$

Now $(\mathbb{Z},+)$ has only one element of finite order

$\Rightarrow G$ has only one element of finite order

Hence correct option is (b)

2. An infinite cyclic group has exactly

(a) one generator (b) two generators (c) three generators (d) four generators **[B.H.U.-2011]**

Soln. We know that every infinite cyclic group has exactly two generators

Correct option is (b)

3. How many elements of the cyclic group of order 8 can be used as generators of the group ?

(a) 2 (b) 3 (c) 4 (d) 5 **[B.H.U.-2011]**

Soln. If G is a cyclic group of order n then the number of generators of G is $\phi(n)$

Given $n = 8$

$\phi(8) = \phi(2^3) = (2^3 - 2^2) = 4$

Correct option is (c)

4. A cyclic group having only one generator can have atmost

(a) 3 elements (b) 4 elements (c) 2 elements (d) 1 element **[B.H.U.-2015]**

Soln. If G is a finite cyclic group of order n then the number of generators of G is $\phi(n)$.

Also $\phi(n) \geq 2$ when $n \geq 3$

Thus if $o(G) = n \geq 3$, then G always have more then one generator

So, we have only two finite groups $\{e\}$ and $\mathbb{Z}_2$ whose number of generators is 1

If G is infinite then we have two generators.

Correct option is (c)

5. The number of elements in the cyclic group $(\mathbb{Z}_{30}, +)$ generated by 24 is : **[B.H.U.-2016]**

(a) 2 (b) 3 (c) 4 (d) 5

Soln. If G is a finite cyclic group. Then the number of elements generated by $x \in G$ is $o(x)$

$\Rightarrow$ The number of elements in the cyclic group $(\mathbb{Z}_{30}, +)$ generated by 24 is $o(24)$

Now, $o(24) = \dfrac{30}{(24,30)} = \dfrac{30}{6} = 5$

Correct option is (d)

6. Which of the following statements isTRUE ? **[B.H.U.-2016]**

(a) In a cyclic group every element is a generator

(b) 1 and 3 are generators of the cyclic group $(\mathbb{Z}_4, +_4)$

(c) Every set of numbers that is a group under addition is also a group under multiplication

(d) Every subset of every group is a subgroup under the induced operation

Soln. For option (a)

Take $G = (\mathbb{Z}_4, +_4) = \{0,1,2,3\}_{+_4}$

Now $2 \in G$

$2^1 = 2$

$2^2 = 2 +_4 2 = 4 = 0$

$\Rightarrow$ 2 is not a generator of G.

$\Rightarrow$ statement (a) is false

For option (b)

If $G = (\mathbb{Z}_4, +_4)$ is a finite cyclic group of order n then $x \in G$ is a generator of G iff $(x,n) = 1$

Now $(1,4) = (3,4) = 1$

$\Rightarrow$ 1 and 3 are generators of the cyclic group $(\mathbb{Z}_4, +_4)$

$\Rightarrow$ statement (b) is true

For option (c)

Take $G = (\mathbb{Z},+)$

Clearly G is a group under addition but not a group under multiplication

$\Rightarrow$ statement (c) is false

For option (d)

Take $G = (\mathbb{Z},+)$

let $H=\{1,-1\}\subseteq G$

Clearly H is not a subgroup of G.

$\Rightarrow$ statement (d) is false

Correct option is (b)

7. In group theory which one of the following statement is correct.

(a) Abelian groups may have non abelian subgroups

(b) Cyclic groups may have non cyclic subgroup **[B.H.U-2017]**

(c) Non abelian groups may have abelian subgroups

(d) Non- cyclic groups can not have cyclic subgroups

Soln. We know that every subgroup of an abelian group is abelian and every subgroup of a cyclic group is cyclic.

$\Rightarrow$ statements (a) and (b) is not correct.

Every proper subgroup of s_3 are of order either 2 or 3.

$\Rightarrow$ Every proper subgroup of s_3 is cyclic.

$\Rightarrow$ statement (c) is correct

Take $G = Q_8$

Clearly G is non cyclic.

But every proper subgroup of G is cyclic.

$\Rightarrow$ statement (d) is incorrect

Correct option is (c)

8. Which of the following groups has a proper subgroup that is not cyclic ?

(a) $\mathbb{Z}_{15}\times\mathbb{Z}_{77}$ (b) S_3 (c) $(\mathbb{Z},+)$ (d) $(\mathbb{Q},+)$

Soln. We know that $\mathbb{Z}_{15}\times\mathbb{Z}_{77}$ and $(\mathbb{Z},+)$ are cyclic groups

$\Rightarrow$ Every proper subgoup of $\mathbb{Z}_{15}\times\mathbb{Z}_{77}$ and $(\mathbb{Z},+)$ is cyclic.

Also every proper subgroup of S_3 is of order either 2 or 3.

$\Rightarrow$ Every proper subgroup of S_3 is cyclic

$\Rightarrow$ option (a), (b) and (b) are incorrect.

Hence correct option is (d)

9. The number of elements of order 6 in a cyclic group of order 36 is equal to **[H.C.U-2015]**

(a) 2 (b) 3 (c) 4 (d) 6

Soln. If G is a cyclic group of order n then the number of elements of order m (where m|n) in G is $\phi\,(m)$.

Thus number of elements of order 6 in a cyclic group of order 36 is ϕ (6) = 2

Correct option is (a).

10. Suppose G is a group and $x \in G$ be such that order of x is $\geq |G|/2$. Then **[H.C.U-2018]**

(a) G is cyclic group
(b) If G is abelian, then G is cyclic
(c) If G is finite, then G is cyclic
(d) none of the above

Soln. By Langrange's theorem we know that if G is a finite group then order of every element of G divides order of G.

Let $G = Q_8$

Let $x = i$

Clearly $o(i) \geq |G|/2$

But G is not an abelian

Hence option (a) and (c) are incorrect

For option (c)

Let $G = K_4$

Clearly $o(a) \geq |G|/2 \; \forall \; a \in G$ and $a \neq e$

Thus G is abelian but not cyclic

Hence option (b) is incorrect

Correct option is (d).

11. The number of subgroups of $\mathbb{Z}_{10}$ is **[H.C.U-2011]**

(a) 1 (b) 2 (c) 3 (d) 4

Soln. The number of subgroups of $\mathbb{Z}_m = \tau(m) =$ the number of positive divisiors of m.

$\Rightarrow$ The number of subgroups of $\mathbb{Z}_{10} = \tau(10) = \tau(2^1 \cdot 5^1) = (1+1)(1+1) = 4$

Correct option is (d)

12. Let G be a cyclic group of order 9. Then **[CUCET-2016]**

(a) G has nine generators
(b) G has six generators
(c) G has five generators
(d) G has three generators

Soln. If G is a finite cyclic group of order n then G has ϕ (n) number of generators.

Given G is a cyclic group of order 9.

$\Rightarrow$ Number of generators of $G = \phi(9) = (3^2 - 3) = 6$

Correct option is (b)

13. Let G be the cyclic group generated by an element α of order 30. What is the order of α^{18}?

(a) 30 (b) 10 (c) 6 (d) none of these. **[ISI-2015]**

Soln. Given $o(\alpha) = 30$

$$\Rightarrow o(\alpha^{18}) = \frac{o(\alpha)}{(o(\alpha),18)} = \frac{30}{(30,18)} = \frac{30}{6} = 5$$

$$\Rightarrow o(\alpha^{18}) = 5$$

Correct option is (d)

14. Consider the group $\mathbb{Z}_p \times \mathbb{Z}_p$ under addition. The number of cyclic subgroups of order p is

(a) 1 (b) $p-1$ (c) $p+1$ (d) p^2-1 **[H.C.U-2011]**

Soln. The number of cyclic subgroups of order $n = \dfrac{\text{The number of elements of order } n}{\phi(n)}$

Now the number of elements of order p in the group $\mathbb{Z}_p \times \mathbb{Z}_p = p^2 - 1$

$\Rightarrow$ The number of cyclic subgroup of order p in $\mathbb{Z}_p \times \mathbb{Z}_p = \dfrac{p^2-1}{\phi(p)} = \dfrac{p^2-1}{p-1} = p+1$

Correct option is (c)

15. Let G be a finite group with no nontrivial proper subgroups. Then which of the following statements are true? **[H.C.U-2015]**

(a) G is cyclic (b) G is abelian

(c) G is of prime order (d) G is non-abelian

Soln. Given G is a finite group with no non trivial proper subgroups.

Let us assume that G is of composite order

Suppose $o(G) = n$

$\Rightarrow \exists$ a prime number $p < n$ such that $p \mid n$

By Cauchy theorem, $\exists$ an element $x \in G$ such that $o(x) = p$

Let $H = \langle x \rangle$

Now H is a proper subgroup of G, which is not possible.

$\Rightarrow o(G)$ is not a composite number

$\Rightarrow o(G)$ is a prime number

$\Rightarrow G$ is cyclic and abelian

Correct option are (a), (b), (c)

16. Which of the following statements are true ? **[NBHM-2013]**

(a) Every group of order 11 is cyclic

(b) Every group of order 111 is cyclic

(c) Every group of order 1111 is cyclic

Soln. For option (a)

We know every group of prime order is cyclic $\Rightarrow$ group of order 11 is cyclic

For option (b)

$111 = 3 \times 37$

Now 3 divides (37–1)

$\Rightarrow$ There is a non abelian group of order 111.

For option (c)

$1111 = 11 \times 101$

Now 11 does not divides (101–1)

$\Rightarrow$ There is only one subgroup of order 1111, which is cyclic.

Hence correct option is (a) and (c).

17. What is the order of the subgroup generated by 25 (mod 30) in the cyclic group $\mathbb{Z}_{30}$? **[NBHM-2005]**

Soln. The order of the subgroup generated by 25 (mod 30) is $o(25)$ in $\mathbb{Z}_{30}$.

Now $o(25)=\dfrac{30}{\gcd(25,30)}=6$

Hence correct answer is (6)

18. Let G be a cyclic group of order 8. How many of the elements of G are generators of this group ? **[NBHM-2008]**

Soln. We know that if G is a cyclic group of order n then the number of generators of G is $\phi(n)$

Here $n = 8$

$\phi(n)=4$

Hence correct answer is (4)

19. The multiplicative group $\mathbb{F}_7^{\times}$ is isomorphic to a subgroup of the multiplicative group $\mathbb{F}_{31}^{\times}$. **[TIFR-2018]**

Soln. $\mathbb{F}_{31}^{\times}=\{1,2,3,\ldots\ldots.30\}_{\times_{31}}$

and $\mathbb{F}_7^{\times}=\{1,2,\ldots\ldots.6\}_{\times_7}$

$\Rightarrow$ $\mathbb{F}_{31}^{\times}$ is a multiplicative group of order 30 i.e.

$\mathbb{F}_{31}^{\times}=U(30)\approx\mathbb{Z}_{30}$

$\Rightarrow$ $\mathbb{F}_{31}^{\times}$ is a cyclic group.

Similarly $\mathbb{F}_7^{\times}\approx\mathbb{Z}_6$ is also cylic.

Now for each divisor of 30, $\mathbb{F}_{31}^{\times}$ has unique cyclic subgroup of that divisor

$\Rightarrow$ $\mathbb{F}_{31}^{\times}$ has a cyclic subgroup of order 6.

Hence statement is true.

20. The number of solutions of $X^5\equiv 1(\text{mod}\,163)$ in $\mathbb{Z}_{163}$ is **[H.C.U-2011]**

(a) 1 (b) 2 (c) 3 (d) 4

Soln. The number of solutions of $X^5\equiv 1(\text{mod}163)$ in $\mathbb{Z}_{163}$ is the number of elements of order 5 in $U(163)$ and one is identity element in $U(163)$.

But $5\nmid 162$.

$\Rightarrow U(163)$ does not have any element of order 5

Also $1^5\equiv 1(\text{mod}\,163)$

Hence correct option is (a)

21. Let G_1 be an abelian group of order 6 and $G_2=S_3$. Let $j=1,2$, P_j be the statement G_j has a unique subgroup of order 2. Then

(a) Both P_1 and P_2 hold (b) Neither P_1 nor P_2 hold

(c) P_1 holds but not P_2 (d) P_2 holds but not P_1

Soln. $G_1\approx\mathbb{Z}_6$ as $2\,\|G|$ as G is cyclic

By theorem on cyclic group there exist a unique subgroup of order 2.

$G_2=S_3$ then $H_1=\{(1),(12)\}$, $H_2=\{(1),(1,3)\}$, $H_3=\{(1),(2,3)\}$

H_1,H_2,H_3 all are cyclic so it is not unique. Hence P_1 hold P_2 does not hold.

Hence, correct option is (c).

22. The value of α for which $G = \{\alpha, 1, 3, 9, 19, 27\}$ is cyclic group under multiplication modulo 56 is

(a) 5 (b) 15 (c) 25 (d) 35

Soln. By the definition of group. It is closed under multiplication modulo 56 so

$3.27 \in G \Rightarrow 81 \bmod 56 \in G \Rightarrow 25 \in G$ so $\alpha = 25$

Hence, correct option is (c).

23. Let G be a group of order 49. Then

(a) G is abelian (b) G is cyclic (c) G is non-abelian (d) center of G has order 7

Soln. Using the result that every group of order p^2 is abelian where p is a prime. Here $p = 7$ then group of order 49 is abelian.

Hence, correct option is (a).

24. Any subgroup of $(\mathbb{Q}, +)$ is

(a) cyclic and finitely generated but not abelian and normal

(b) cyclic and abelian but not finitely generated and normal

(c) abelian and normal but not cyclic and finitely generated

(d) finitely generated and normal but not cyclic and abelian

Soln. As $(\mathbb{Q}, +)$ is abelian so any subgroup of $(\mathbb{Q}, +)$ is abelian. So (a) and (d) are contradiction. Every subgroup of abelian group is normal. So (b) is contradiction.

Hence, correct option is (c).

25. Consider the following statement

S : Every non-abelian group has a non-trivial abelian subgroup

T : Every non-trivial abelian group has a cyclic subgroup then

(a) both S and T are false (b) S is true and T is false

(c) T is true and S is false (d) both S and T are true

Soln. For S let G be non-abelian group then take $H = \{e, a\}$ where $a \in G$ and $a = a^{-1}$ or $H = \{e, a, b\}$ where $a, b \in G$ and $ab = e = ba$ in both case H is non-trivial and abelian. Hence S is true.

For T let G be non-trivial abelian group take $H = \{e\}$ which is cyclic. Hence T also true.

Both S and T are true.

Hence, correct option is (d).

26. All non-trivial proper subgroup of $(\mathbb{R}, +)$ are cyclic. True or False ? **[TIFR-2013]**

Ans. False

Soln. Let proper subgroup of $(\mathbb{R}, +)$ is $(\mathbb{Q}, +)$ which is not cyclic.

Hence statement is false.

27. A cyclic group of order 60 has

(a) 12 generator (b) 15 generator (c) 16 generator (d) 20 generator **[TIFR-2010]**

Soln. Number of generator in a cyclic group of order n is $\phi(n)$

here $n = 60 \Rightarrow \phi(60) = 60 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16.$

Hence, correct option is (c).

28. In a non abelian group the element 'a' has order 108, then order of a^{42} is

(a) 54 (b) 27 (c) 18 (d) 9

Soln. $o(a^k) = \dfrac{o(a)}{\gcd\left(o(a), k\right)} = \dfrac{108}{\gcd(108, 42)} = \dfrac{108}{6} = 18$

Hence, correct option is (c).

29. The number of subgroups of the group $\mathbb{Z}_{200}$ is

(a) 8 (b) 14 (c) 12 (d) 10 **[D.U. 2015]**

Soln. The number of subgroups of the group $\mathbb{Z}_{200}$ is number of divisors of 200.

So, $\tau(200) = \tau(2^3 \times 5^2) = (3+1)(2+1) = 4 \times 3 = 12$

Hence, correct option is (c)

30. Which of the following is /are true ?

(a) Let G be a group such that $|G| = mn, m > 1, n > 1$. Then G has a non trivial subgroup.

(b) If G be an infinite cyclic group generated by a, then $a^r = a^t$ iff $r = t$, $r, t \in \mathbb{Z}$

(c) Let G be a group such that $|G| = mn, m > 1, n > 1,$ then G need not to have a non trivial subgroup

(d) None of these

Soln. For option (a)

Suppose G is cyclic Let $G = \langle a \rangle$, then $o(a) = mn$

Clearly $o(a^m) = n$ Let $H = \langle a^m \rangle$. Thus H is a non trivial subgroup of G.

Now suppose G is not cyclic then $\forall a \in G$, $o(a) \neq mn$

Let $e \neq a$ and let $H = \langle a \rangle$

then H is non trivial subgroup of G

$\therefore$ option (a) is correct and (c) is false

For option (b)

Suppose $a^r = a^t$ and $r \neq t$ Let $r > t$ then $a^{r-t} = e$

Thus o (a) is finite say $o(a)=n$. then $G = \{e, a, a^2 .... a^{n-1}\}$

which is a contradiction.

Since G is an infinite group and convers is also true

So option (b) is correct

Correct option is (a), (b)

31. Let a and b belong to group G. If $|a| = 12$, $|b| = 22$ and $\langle a \rangle \cap \langle b \rangle \neq \{e\}$. Then

(a) $a^3 = a^{11}$ (b) $a^6 = a^{11}$ (c) $a^4 = a^{11}$ (d) None of these

Soln. Since $\langle a \rangle \cap \langle b \rangle$ is subgroup of $\langle a \rangle$ and $\langle b \rangle$. so $|\langle a \rangle \cap \langle b \rangle|$ divides 12 and 22.

$\Rightarrow |\langle a \rangle \cap \langle b \rangle| = 1$ or 2 and since

$|\langle a \rangle \cap \langle b \rangle| \neq \{e\}$ we have $|\langle a \rangle \cap \langle b \rangle| = 2$

Because $\langle a^6 \rangle$ is the only subgroup of $\langle a \rangle$ of order 2 and $\langle b^{11} \rangle$ is the only subgroup of $\langle b \rangle$ of order 2.

We have $\langle a \rangle \cap \langle b \rangle = \langle a^6 \rangle = \langle b^{11} \rangle$

$\therefore \boxed{a^6 = b^{11}}$

Option (b) is correct

32. Let $a^5 = 1$ and $a^{-1}ba = b^m$ in a group G, then

(a) $b^{m^6} - 1$ (b) $b^{m^5} - 1$ (c) $b^{m^4} - 1$ (d) None of these

Soln. Let $a^5 = 1$ and $a^{-1}ba = b^m$ then

$$a^{-2}ba^2 = a^{-1}b^m a = \left(a^{-1}\,ba\right)^m$$

$$= \left(b^m\right)^m = b^{m^2}$$

Next, $a^{-3}ba^3 = a^{-1}b^{m^2}a = \left(a^{-1}ba\right)^{m^2} = \left(b^m\right)^{m^2} = b^{m^3}$

Similarly, $a^{-4}ba^4 = b^{m^4}$ and finally $b = a^{-5}ba^5 = b^{m^5} \Rightarrow b^{m^5-1} = 1$

Correct option is (b)

33. Which of the follwing is/are true ?

(a) If $G = \langle a \rangle$ is cyclic, then subgroup $H = \left\{\langle x, y \rangle : x = a^4, y = a^3\right\}$ equal G.

(b) If $G = \langle a \rangle$ is cyclic and a subgroup $H = \left\{\langle x, y \rangle : x = a^4, y = a^3\right\}$ need not to be equal to G.

(c) If $G = \langle a \rangle$ is cyclic. then subgroup $H = \left\{\langle x, y \rangle : x = a^m\, y = a^k\right\}$ is subgroup generated by $\left\langle a^d\ ; g.c.d\left(m, k\right) = d\right\rangle$ i.e. $\left\langle a^d \right\rangle$

(d) None of these

Soln. We have $a = a^4\left(a^3\right)^{-1} \in H$, So $G = \langle a \rangle \subseteq H$

Thus H = G

option (a) is correct and (b) is false

For (c) we have $d = xm + yk$ with $x, y \in Z$

So $a^d = \left(a^m\right)^x \left(a^k\right)^y \in H$

Thus $\left\langle a^d \right\rangle \subset H$ But d|m so $m = qd$

So $a^m = \left(a^d\right)^q \in \left\langle a^d \right\rangle$

Similarly $a^k \in \left\langle a^d \right\rangle$ so $\boxed{H = \left\langle a^d \right\rangle}$

option (c) is also correct

Correct option is (a) and (c)

Chapter 4

PERMUTATION GROUP

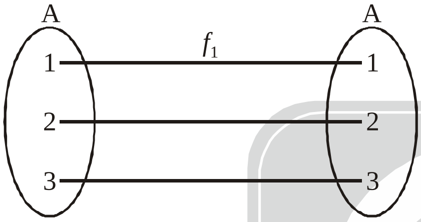
Permutation of *A*, Permutation Group of *A* :

A permutation of a set *A* is a function from *A* to *A* that is both one to one and onto.

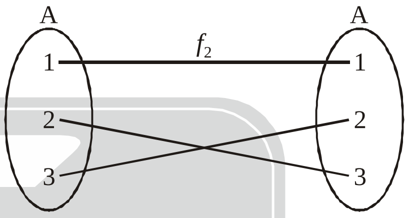
A permutation group of a set is a set of permutations of *A* that forms a group under function composition.

Ex. Let $A = \{1, 2, 3\}$. Then if we define all one-one onto functions from *A* to *A*. There will be total 6 possibilities as

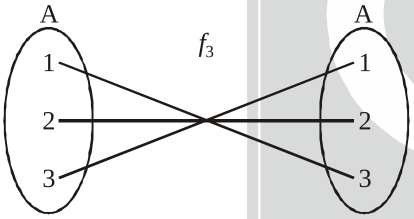
(1)



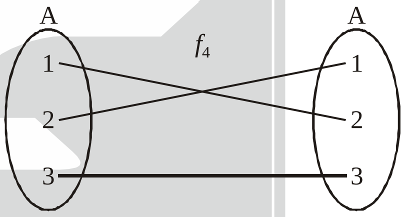
(2)



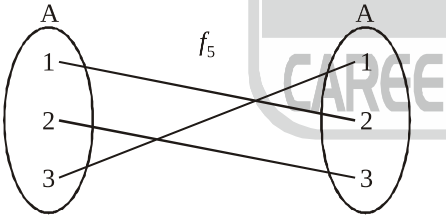
(3)



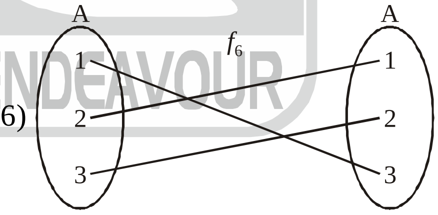
(4)



(5)



(6)



So, there are total 6 one-to-one onto homomorphism from *A* to *A*.

For example, we define a permutation α of the set {1, 2, 3, 4} by specifying

$\alpha(1) = 2,$ $\alpha(2) = 3,$ $\alpha(3) = 1,$ $\alpha(4) = 4$.

A more convenient way to express this correspondence is to write α in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

Here $\alpha(j)$ is placed directly below *j* for each *j*. Similarly, the permutation β of the set $\{1, 2, 3, 4, 5, 6\}$ given by

$\beta(1) = 5,\ \beta(2) = 3,\ \beta(3) = 1,\ \beta(4) = 6,\ \beta(5) = 2,\ \beta(6) = 4$

is expressed in array form as $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$

2. **Equality of two permutations:** Two permutations f and g of degree n are said to be equal if we have $f(a) = g(a)\,\forall\, a \in S$.

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ are two permutations of degree 4, then we have $f = g$. Here we see that both f and g replace 1 by 2, 2 by 3, 3 by 4 and 4 by 1.

If $f = \begin{pmatrix} a_1 & a_2 & a_3 ... & a_n \\ b_1 & b_2 & b_3 ... & b_n \end{pmatrix}$ is a permutation of degree n, we can write it in several ways. The interchange of columns will not change the permutation. Thus we can write.

$$f = \begin{pmatrix} a_2 & a_1 & a_3 ... & a_n \\ b_2 & b_1 & b_3 ... & b_n \end{pmatrix} = \begin{pmatrix} a_n & a_1 ... & a_2 \\ b_n & b_1 ... & b_2 \end{pmatrix} = \begin{pmatrix} a_n & a_{n-1} ... a_2 & a_1 \\ b_n & b_{n-1} ... b_2 & b_1 \end{pmatrix} \text{ etc.}$$

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ are two permutations of degree 4, then by interchanging columns we can write $g = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

3. **Total number of distinct permutations of degree *n*.** If S is a finite set having n distinct elements, then we shall have $n!$ distinct arrangements of the elements of S. Therefore there will be $n!$ distinct permutations of degree n. If S_n be the set consisting of all permutations of degree n, then the set S_n will have $n!$ distinct elements. This set S_n is called the symmetric set of permutations of degree n. Thus

$S_n = \{f : f \text{ is a permutation of degree } n\}$.

The set S_3 of all permutations of degree 3 will have 3! i.e., 6 elements. Obviously

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

4. **Identity Permutation:** If I is a permutation of degree n such that I replaces each element by the element itself, I is called the identity permutation of degree n.

Thus, $I = \begin{pmatrix} 1 & 2 & 3...n \\ 1 & 2 & 3...n \end{pmatrix}$ or $\begin{pmatrix} a_1 & a_2 & a_3 ... a_n \\ a_1 & a_2 & a_3 ... a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 & b_3 ... b_n \\ b_1 & b_2 & b_3 ... b_n \end{pmatrix}$

is the identity permutation of degree n.

5. **Product or composite of two permutations:** The product or composition of two permutations f and g of degree n denoted by fg, is obtained by first carrying out the operation defined by g and then by f.

For example, Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$ and $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$ then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

6. Groups of Permutations:

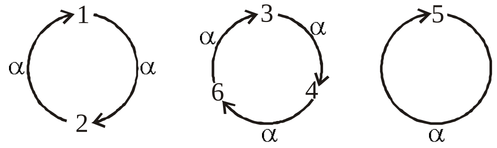
Theorem: The set S_n of all permutations on n symbol is a finite group of order $n!$ with respect to composition of mappings as the operation. For $n \le 2$, this group is abelian and for $n > 2$ it is always non-abelian.

7. Cycle Notation: There is another notation commonly used to specify permutations. It is called cycle notation and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical advantages in that certain important properties of the permutation can be readily determined when cyclic notation is used.

As an illustration of cycle notation, let us consider the permutation.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$

This assignment of values could be presented schematically as follows:



We can simply write $\alpha = (1\ 2)(346)(5)$. As second example, consider

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

In cycle notation, β can be written (2 3 1 5) (6 4) or (4 6) (3 1 5 2). An expression of the form $(a_1, a_2, ..., a_m)$ is called a cycle of length m or an m-cycle.

8. Permutations represented by a cycle: (1 3 4 2 6) is a cycle of length 5. Suppose it represents a permutation of degree 9 on a set S consisting of the elements 1, 2,...,9. Then the permutation represented will be

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

i.e., the image of each element in the cycle (1 3 4 2 6) is the element which follows it, the image of the last element 6 is the first element 1 and the missing elements 5, 7, 8, 9 are their images themselves. However, if the cycle (1 3 4 2 6) represents a permutation of degree 6 on six symbols 1, 2, 3, 4, 5, 6 then the corresponding permutation will be

$$\begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 \\ 3 & 4 & 2 & 6 & 1 & 5 \end{pmatrix}$$

Important Note: A cycle does not change by changing the places of its elements provided their cyclic order is not changed.

Thus (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3)

Also (1 2) = (2 1), (2 3) = (3 2).

9. Transpositions. Definition: A cycle of length two is called a transposition. Thus the cycle (1 3) is a transposition. If the transposition (2, 3) is a permutation of degree 3 on three symbols 1, 2, 3 then the corresponding permutation will be

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

A cycle of length one means that the image of the element involved is the element itself and the missing elements are left unchanged. Thus all the elements are left unchanged. Therefore every cycle of length one will represent the identity permutation.

10. **Multiplication of Cycles.** We multiply cycles by multiplying the permutations represented by them. For example if the cycles (1 2 3) and (5 6 4 1) represent permutation of degree 6 on six symbols, 1, 2, 3, 4, 5, 6, then

$$(5\ \ 6\ \ 4\ \ 1)\ \ (1\ \ 2\ \ 3) = \begin{pmatrix} 5 & 6 & 4 & 1 & 2 & 3 \\ 6 & 4 & 1 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 6 & 4 \end{pmatrix} = (1\ \ 2\ \ 3\ \ 5\ \ 6\ \ 4)$$

Since, a cycle of length one represents the identity permutation, therefore (1) (2 3 4) (6) = (2 3 4).

11. **Disjoint Cycles:** Two cycles are said to be disjoint if they have no symbol in common. For example (123) and (45) are disjoint cycles

Theorem: If *f* and *g* are two disjoint cycles, then $fg = gf$ i.e., the product of disjoint cycles is commutative.

Proof : The cycles *f* and *g* have no symbols common. Therefore the elements permuted by *f* are left unchanged by *g* and also the elements permuted by *g* remain the same under *f*. Therefore we shall have $fg = gf$.

Now we shall give an example to illustrate this theorem. Let $f = (1\ 2\ 3)$ and $g = (4\ \ 5)$ represent two permutation on 5 symbols 1, 2,...,5.

$$\text{Then } gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

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

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

$$= (1\ \ 2\ \ 3)(4\ \ 5) = fg$$

Inverse of a cyclic permutation: To prove that $(1\ \ 2\ \ 3...n)^{-1} = (n\ n-1...3\ 2\ 1)$ i.e., to write the inverse of a cycle we should write its elements in the reverse order.

Proof : We have $(1\ \ 2\ \ 3...n)(n...3\ \ 2\ \ 1)$

$$= \begin{pmatrix} 1 & 2 & 3...n-1 & n \\ 2 & 3 & 4...n & 1 \end{pmatrix}\begin{pmatrix} n & ...4 & 3 & 2 & 1 \\ n-1 & ...3 & 2 & 1 & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3...n-1 & n \\ 1 & 2 & 3...n-1 & n \end{pmatrix} = I$$

Also $(n...3\ \ 2\ \ 1)\ (1\ \ 2\ \ 3...n) = I$

$$\therefore\ (1\ \ 2\ \ 3...n)^{-1} = (n...3\ \ 2\ \ 1)$$

In particular, every transposition is its own inverse. If (1 2) is a transposition, then $(1\ \ 2)^{-1}$ = (2 1) = (1 2).

Inverse of a product of cyclic permutations. If *f* and *g* are any two cycles, then we have

$(fg)^{-1} = g^{-1}f^{-1}$. Also $(fgh)^{-1} = h^{-1}g^{-1}f^{-1}$

If *f* and *g* are disjoint cycles then $(fg)^{-1} = (gf)^{-1} = f^{-1}g^{-1}$

Thus $[(1\ \ 2\ \ 3)(4\ \ 5)(7\ \ 6)]^{-1} = (7\ \ 6)^{-1}\ (4\ \ 5)^{-1}\ (1\ \ 2\ \ 3)^{-1}$

$= (6\ \ 7)\ (5\ \ 4)\ (3\ \ 2\ \ 1)$

Also, $[(1\ \ 3\ \ 5)(2\ \ 4)]^{-1} = (1\ \ 3\ \ 5)^{-1}\ (2\ \ 4)^{-1} = (5\ \ 3\ \ 1)\ (4\ \ 2)$.

We shall now give some important results on the product of permutations.

12. **Theorem: Products of Disjoint Cycles:** Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Ex. Write to the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 5 & 8 & 6 & 2 & 1 \end{pmatrix}$ **in disjoint cycles.**

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

Remarks :

(*i*) 1-cycles does not effect to the permutation if we do not write them in product of disjoint cycles.

(*ii*) We can express above expression in transpositions as $\begin{pmatrix} 1 & 4 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 8 \end{pmatrix}$

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

13. **Theorem: Disjoint cycles commute:** If the pair of cycles $\alpha = (a_1, a_2, ..., a_m)$ and $\beta = (b_1, b_2, ..., b_n)$ have no entries in common then $\alpha\beta = \beta\alpha$.

14. **Theorem: Order of a Permutation (Ruffini-1799):** The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof: First, observe that a cycle of length *n* has order *n*. (Verify this yourself). Next, suppose that α and β are disjoint cycles of lengths *m* and *n*, and let *k* be the least common multiple of *m* and *n*. It follows from theorem that both α^k and β^k are the identity permutation *e* and, since α and β commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus, we know that $a^k = e$ implies that $o(a)$ divides *k*.

$\Rightarrow$ The order of $\alpha\beta$ - let us call it '*t*' must divide *k*. But then $(\alpha\beta)^t = \alpha^t\beta^t = e$, so that $\alpha^t = \beta^{-t}$. However, it is clear that if α and β have no common symbol, the same is true for α^t and β^{-t}, since raising a cycle to a power does not introduce new symbols. But, if α^t and β^{-t} are equal and have no common symbols, they must both be the identity, because every symbol in α^t is fixed by β^{-t} and vice versa (remember that a symbol not appearing in a permutation is fixed by the permutation). It follows, then, that both *m* and *n* must divide *t*. This means that *k*, the least common multiple of *m* and *n*, divides *t* also. This shows that *k* = *t*.

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

15. **Theorem: Product of 2-cycles:** Every permutation in $S_n, n > 1$, is a product of 2-cycles.

Proof: First, note that the identity can be expressed as (12) (12)

We know that every permutation can be written in the form $(a_1a_2...a_k)(b_1b_2...b_t)...(c_1c_2...c_s)$

Direct computation shows that this is the same as

$(a_1a_k)(a_1a_{k-1})...(a_1a_2)(b_1b_t)(b_1b_{t-1})...(b_1b_2)...(c_1c_s)(c_1c_{s-1})...(c_1c_2)$

This completes the proof.

The first decomposition in the following example demonstrates this technique. The other products in example show that the decomposition on permutation into a product of 2-cycles is not unique.

Example: (12345) = (15) (14) (13) (12)
= (45) (53) (25) (15)
= (21) (25) (24) (23)
= (54) (52) (21) (25) (23) (13)

Definition: Even and Odd Permutations: A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.

Theorems together show that every permutation can be unambiguously classified as either even or odd, but not both. At this point, it is natural to ask what significance this observations has. The answer is given in theorem.

Ex. (*i*) Identity permutation is always an even permutation.

(*ii*) Any transposition is always an odd permutation.

(*iii*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$ odd or even ??

Soln. $(1\ \ 2\ \ 6\ \ 3)\,(4\ \ 5) = (1\ \ 2)\,(1\ \ 6)\,(1\ \ 3)\,(4\ \ 5)$

since given permutation can be expressed as product of even number of transpositions. Hence given permutation is an even permutation.

16. **Lemma:** If $e = \beta_1\beta_2...\beta_r$ where the $\beta'r$ are 2-cycles, then r is even.

17. **Theorem: Always even or always odd:** If a permutation α can be expressed as a product of an even number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even number of 2-cycles. In symbols, if

$\alpha = \beta_1\beta_2...\beta_r$ and $\alpha = \gamma_1\gamma_2...\gamma_s$,

where the $\beta's$ and the $\gamma's$ are 2-cycles, then r and s are both even or both odd.

Proof : Observe that $\beta_1\beta_2...\beta_r = \gamma_1\gamma_2...\gamma_s$ implies

$e = \gamma_1\gamma_2...\gamma_s\beta_r^{-1}...\beta_2^{-1}\beta_1^{-1} = \gamma_1\gamma_2...\gamma_s\beta_r...\beta_2\beta_1$

since, a 2-cycle is its own inverse. Thus, the lemma above guarantees that $s + r$ is even. It follows that r and s are both even or both odd.

18. **Theorem:** A permutation cannot be both even and odd i.e., if a permutation f is expressed as a product of transpositions then the number of transpositions is either always even or always odd.

19. **Cor.1.** A cycle of length n can be expressed as a product of n–1 transpositions. Therefore a cycle of length n will be an even permutation if n is odd and it will be an odd permutation if n is even.

In particular, every transposition is an odd permutation.

20. **Cor.2.** Identity permutation is always an even permutation.

If I is the identity permutation then I can be expressed as the product of two transpositions. For example we can write

I = (1 2) (2 1).

Therefore, I is an even permutation

21. **Cor.3.** The product of two even permutations is an even permutation.

Suppose f and g are two even permutations. Further suppose that f can be expressed as the product of r transpositions and g can be expressed as the product of s transpositions. Then r and s are both even. Now fg can be expressed as the product of $r + s$ transpositions. Since $r + s$ is even, therefore fg is an even permutation.

22. **Cor.4.** The product of two odd permutations is an even permutation.

23. **Cor.5.** The product of an even permutation and an odd permutation is an odd permutation. Similarly the product of an odd permutation and an even permutation is an odd permutation.

24. **Cor. 6.** The inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation.

Suppose f is an even permutation. If f^{-1} is the inverse of f, then $f^{-1} f = I$ (identity permutation).

Now I is an even permutation and f is also an even permutation. Therefore, f^{-1} cannot be an odd permutation otherwise $f^{-1} f$ will be an odd permutation. Hence f^{-1} is an even permutation.

Similarly, if f is an odd permutation, then f^{-1} must also be an odd permutation.

25. **Theorem:** Out of the $n!$ permutations on n symbols, $\frac{1}{2}n!$ are odd permutations.

Proof : Out of $n!$ permutations on n symbols let the even permutations be $e_1, e_2, ..., e_m$ and the odd permutations be $o_1, o_2, ..., o_k$.

Since, a permutation is either an even permutation or an odd permutation but not both, therefore $m + k = n!$
If S_n be the set of all permutations of degree n, then

$S_n = \{e_1, e_2, ..., e_m, o_1, o_2, ..., o_k\}$

Let $t \in S_n$ and suppose t is a transposition.

Since, S_n is a group with respect to permutation multiplication, therefore $te_1, te_2, ..., te_m, to_1, to_2, ..., to_k$ are all elements of S_n. Obviously $te_1, te_2, ..., te_m$ are all odd permutations and $to_1, to_2, ..., to_k$ are all even permutations.

Now no two of the permutations $te_1, te_2, ..., te_m$ are equal because

$te_i = te_j \Rightarrow e_i = e_j$ (by left cancellation law in the group S_n).

Therefore, if $e_i \neq e_j$, then $te_i \neq te_j$.

Thus, the m odd permutations $te_1, ..., te_m$ are distinct elements of S_n. But we have supposed that S_n contains exactly k odd permutations. Therefore m cannot be greater than k. Thus

$m \le k$ ...(1)

Similarly, we can show that the k even permutations $to_1, to_2, ..., to_k$ are distinct elements of S_n. Therefore, we must have

$k \le m$ ...(2)

From (1) and (2), it follows that $m = k = \frac{n!}{2}$.

Note: If A_n is the set of all even permutations of degree n then $A_n \subset S_n$ and A_n contains $\frac{n!}{2}$ elements. The set A_n is called an alternating set of permutations of degree n.

26. **Theorem:** The set A_n of all even permutations of degree n forms a finite group of order $\frac{n!}{2}$ with respect to permutation multiplication.

Proof : The product of two even permutations is also an even permutation. Therefore, the set A_n is closed with respect to multiplication of permutations as composition.
We know that multiplication of permutations is an associative composition.

If I is the identity permutation of degree n then I is an even permutation. Therefore $I \in A_n$. Now we have

$If = f = fI \; \forall \; f \in A_n$

$\therefore$ I is the identity element.

Let f be any permutation of degree n. If f^{-1} is the inverse of f in the group of all permutations of degree n, then f^{-1} is also an even permutation because $f^{-1}f = I$ (an even permutation).

Thus $f \in A_n \Rightarrow$ then there exists $f^{-1} \in A_n$ such that $f^{-1}f = I = ff^{-1}$.
Therefore, every element of A_n possesses inverse.

The total number of all even permutations of degree n is $\frac{n!}{2}$. Thus there are $\frac{n!}{2}$ elements in the set A_n.

$\therefore$ A_n forms a finite group of order $\frac{n!}{2}$ with respect to multiplication of permutations.

Note: The product of two odd permutations is an even permutation. Therefore the set of all odd permutations is not closed with respect to multiplication. Therefore it will not be a group.

Ex.1. Write the following permutations as the product of disjoint cycles.

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

(b) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

Soln. (a) We have $f = (6)\ (7)\ (1\ 2\ 3\ 4\ 5)\ (8\ 9)$ or $f = (1\ 2\ 3\ 4\ 5)\ (8\ 9)$, omitting cycles of length 1 as they represent identity permutations.

(b) We have $g = (1\ 6\ 2\ 5)(3\ 4)$.

SUMMARY : PERMUTATION GROUPS

1. Let S be a non-empty set and σ be a permutation on S. For $a, b \in S$ define a relation ~ on S by $a \sim b \Leftrightarrow \sigma^n$ $(a) = b$ for some integer n. This relation ~ is an equivalence relation.

2. S_n is a Non-abelian group for $\forall\ n > 2$

3. Every $\sigma \in S_n$ can be expressed as a product of disjoint cycles

4. Every r-cycle can be express as product of $r-1$ transpositions

5. If $\sigma \in S_n$ be a r-cycle then σ is even permutation if r is odd and odd permutation if r is even

6. If H is a subgroup of S_n then either H consists of all even permutations or exactly half of them are even

7. The symmetric group S_n is generated by $n-1$ transposition $(1\quad 2), (1\quad 3), \ldots (1\quad n)$

8. The group S_n is generated by the cycles $\sigma = (1\,2\,3 \ldots n)$ and $\gamma = (1\quad 2)$

9. The alternating group A_n $(n \geq 3)$ may be generated by $n-2$, 3 cycles $(1\ \ 2\ \ 3), (1\ \ 2\ \ 4), \ldots, (1\ \ 2\ \ n)$

10. The number of r-cycles in a symmetric group on n-symbols (in S_n) is given by $\dfrac{{}^nP_r}{r}$

Ex. ***(i)*** How many elements of 2-cycle in S_3 ??

Soln. Number of elements of 2-cycle $= \dfrac{3!}{2 \times (3-2)!} = \dfrac{6}{2} = 3$

And elements are $(1\,2), (2\,3), (3\,1)$

(ii) The distinct cycle decomposition of permutations in S_n are same as number of partitions of n.

12. If $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_q\}$ then order of $o(\sigma) = l.c.m.\ \{n_1, n_2, \ldots, n_q\}$

13. Let $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_k\}$ and let α_i is number of cycles of length i and $\{n_1, n_2, \ldots, n_k\}$ such that $\sum_{i=1}^{n} n_k = n$ then number of elements similar to σ or number of permutations whose order is same as order of $\sigma = \dfrac{n!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot 3^{\alpha_3} \ldots\ldots n^{\alpha_k} \cdot \alpha_1! \cdot \alpha_2! \ldots\ldots \alpha_k!}$

Solved Examples

1. Let $\sigma = (37125)(43216) \in S_7$, the symmetric group of degree 7. The order of σ is **[DU-2018]**

(a) 7 (b) 4 (c) 5 (d) 2

Soln. Given $\sigma = (37125)(43216) = (4716)(2)(35)$

$\Rightarrow o(\sigma) = 4$

Hence correct option is (b)

2. The number of elements in the alternating group A_5 is

(a) 15 (b) 30 (c) 60 (d) 120 **[B.H.U.-2011]**

Soln. We know that $o(A_n) = \dfrac{n!}{2}$

$\Rightarrow o(A_5) = \dfrac{5!}{2} = 60$

Hence correct option is (c)

3. The number of odd permutations of the set {1, 3, 5, 7, 9} is

(a) 15 (b) 30 (c) 60 (d) 120 **[B.H.U.-2012]**

Soln. We know that the number of odd permutations on n symbols $= \dfrac{n!}{2}$

$\Rightarrow$ The number of odd permutations of the set $\{1,3,5,7,9\} = \dfrac{5!}{2} = 60$

Hence correct option is (c)

4. Which power multiplying itself of the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ gives $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$?

(a) f (b) f^2 (c) f^3 (d) f^4 **[B.H.U.-2012]**

Soln. Given $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (234)$

Clearly $o(f) = 3$

Hence correct option is (c)

5. What is the number of disjoint cycles of length >1 in the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 7 & 6 & 3 & 4 & 1 \end{pmatrix}$?

(a) 2 (b) 3 (c) 4 (d) 5 **[B.H.U-2017]**

Soln. We can write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 7 & 6 & 3 & 4 & 1 \end{pmatrix}$ as $(1537)(46)(2)$

Thus number of disjoint cycles of length > 1 is 2

Hence correct option is (a)

6. Total number of transpositions in the permutation **[B.H.U-2018]**

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 3 & 5 & 1 & 6 & 8 & 2 & 7 & 4 \end{pmatrix}$ are

(a) 8 (b) 7 (c) 9 (d) 6

Soln. Given $f=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 3 & 5 & 1 & 6 & 8 & 2 & 7 & 4 \end{pmatrix}$

$=(110\ 4\ 5)(2\ 9\ 7\ 8)(3)(6)$

$=(110)(14)(15)(29)(27)(28)$

Thus total number of transpositions in the permutation $f=6$

Hence correct option is (d)

7. The converse of the lagrange's theorem for a group does not hold in the

(a) Klein's four group V_4 (b) Hamiltonian group Q_8 **[B.H.U-2017]**

(c) Symmetric Group S_3 (d) Alternating group A_4

Soln. The converse of lagrange's theorem does not hold in the alternating group A_4.

Hence correct option is (d)

8. Let S_{10} denote the group of permutations on ten symbols $\{1, 2, ..., 10\}$. The number of elements of S_{10} commuting with the element $\sigma = (1\ 3\ 5\ 7\ 9)$ is

(a) 5! (b) $5\cdot 5!$ (c) 5! 5! (d) 10!/5!

Soln. Given $\sigma=(1\,3\,5\,7\,9)$

We know that if σ is *m* cycle on *n* symbols then the number of elements of S_n commuting with the element

$$\sigma=\frac{n!}{\text{Number of cycles of length } m}$$

The number of elements of S_{10} commuting with the element $\sigma(=(13579))=\dfrac{10!}{\dfrac{10!}{5!\cdot 5}}=5.5!$

Hence correct option is (b)

9. In the permutation group S_6, the number of elements of order 8 is

(a) 0 (b) 1 (c) 2 (d) 4

Soln. No partition of 6 have lcm 8

$\Rightarrow$ The number of elements of order 8 is 0

Hence correct option is (a)

10. The order of (123)(145) in the permutation group S_5 is **[H.C.U.-2018]**

(a) 6 (b) 3 (c) 5 (d) 9

Soln. Given $\sigma=(1\,2\,3)(1\,4\,5)=(1\,4\,5\,2\,3)$

$\Rightarrow \sigma$ is a 5-cycle

$\Rightarrow o(\sigma)=5$

Hence correct option is (c)

11. The number of subgroups of order 2 in the permutation group S_3 is **[H.C.U.-2018]**

(a) 1 (b) 3 (c) 2 (d) 12

Soln. The number of subgroups of order 2 in any group *G* = The number of elements of order 2 in *G*.

Thus the number of subgroups of order 2 in S_3 = 3

Hence correct option is (b)

12. Let S_9 be the group of all permutations of the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Then the total number of elements of S_9 that commute with $\tau = (1\,2\,3)(4\,5\,6\,7)$ in S_9 equals ________.

Soln. We know that the total number of elements commuting with any permutation σ in S_n is

$$\frac{n!}{\text{Number of elements with the same cycle decomposition of } \sigma}$$

Given $\tau = (1\,2\,3)(4\,5\,6\,7)$

Number of elements with the same cycle decomposition of $\tau = \dfrac{9!}{2!\ 3^1 \cdot 4^1}$

Thus number of elements commuting with $\tau = \dfrac{9!}{9!} \cdot 2! \cdot 3 \cdot 4 = 24$

Hence correct answer is (24)

13. Consider the permutation π given by

$$\begin{array}{cccccccccccc} n & = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \pi(n) & = & 5 & 7 & 8 & 10 & 6 & 1 & 2 & 4 & 9 & 3 \end{array}$$

Find the order of the permutation π. **[NBHM-2007]**

Soln. Given

$$\begin{array}{cccccccccccc} n & = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \pi(n) & = & 5 & 7 & 8 & 10 & 6 & 1 & 2 & 4 & 9 & 3 \end{array}$$

$\Rightarrow \pi = (156)(27)(3\,8\,4\,10)(9)$

$\Rightarrow o(\pi) = \text{1cm}\,\{3, 2, 4, 1\} = 12$

Hence correct answer is (12)

14. Let S_5 denote the symmetric group of all permutations of the five symbols $\{1, 2, 3, 4, 5\}$. What is the highest possible order of an element in this group ? **[NBHM-2012]**

Soln. Partitions of 5 are 1+1+1+1+1, 1+2+2, 1+1+1+2, 2+3, 1+4, 5, 1+1+3 and 5

Now lcm{2, 3} = 6, which is greatest lcm among the partitions of 5.

Thus highest possible order of an element in group S_5 = 6

Hence correct answer is (6)

15. Let S_n denote the symmetric group of order n, i.e. the group of all permutations of the n symbols $\{1, 2,..., n\}$. Given two permutations σ and τ in S_n, we define the product $\sigma\tau$ as their composition got by applying σ first and then applying τ to the set $\{1, 2,..., n\}$. Write down the following permutation in S_8 as the product of distinct cycles: (1 4 3 8 7) (5 4 8). **[NBHM-2013]**

Soln. $(1\ 4\ 3\ 8\ 7)(5\ 4\ 8) = (1\ 8\ 7)(3\ 5\ 4)$

16. Find the sign of the permutation σ defined below: **[NBHM-2014]**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Soln. Given $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$

Clearly σ is an odd permutation

$\Rightarrow$ The sign of permutation σ is negative.

17. The symmetric group S_5 consisting of permutations on 5 symbols has an element of order 6. **[TIFR-2011]**

Soln. Let $\sigma = (1\,2\,3)(4\,5) \in S_5$

Clearly $o(\sigma) = 6$

Thus this statement is True.

18. Let S_7 be the group of permutations on 7 symbols. Does S_7 contain an element of order 10 ? If the answer is "yes", then give an example. **[NBHM-2006]**

Soln. Let $\sigma = (1\ 2\ 3\ 4\ 5)(6\ 7) \in S_7$

Clearly $o(\sigma) = 10$

Thus this statement is True

19. Let $\sigma = (14387)$ and $\tau = (548)$ be cycles in S_8. Express $\sigma\tau$ and $\tau\sigma$ (see, Notations) as the product of disjoint cycles. **[NBHM-2017]**

Soln. $\sigma\tau = (1\ 4\ 3\ 8\ 7)(5\ 4\ 8) = (5\ 3\ 8)(4\ 7\ 1)$ and $\tau\sigma = (5\ 4\ 8)(1\ 4\ 3\ 8\ 7) = (1\ 8\ 7)(3\ 5\ 4)$

20. Let S_{17} be group of all permutations of 17 distinct symbols. How many subgroups of order 17 does S_{17} have? Justify your answer. **[ISI-2016]**

Soln. The number of elements of order 17 in the group $S_{17} = \frac{17!}{17} = 16!$

The number of subgroups of order 17= $\frac{\text{number of elements of order 17}}{\phi(17)} = \frac{16!}{16} = 15!$

21. The number of elements of order 5 in the symmetric group S_5 is

(a) 5 (b) 20 (c) 24 (d) 12

Soln. Number of elements of order 5 in S_5 is $\frac{5!}{5} = 4! = 24.$

Hence, correct option is (c).

22. The symmetric group S_5 consisting of permutations on 5 symbol has an element of order 6. True or False ?

Ans. True **[TIFR-2011]**

Soln. Take σ = (12) (345) then $o(\sigma) = lcm\,(o(12), o(345)) = lcm\,\{2, 3\}$

$\Rightarrow o(\sigma) = 6.$

Hence true statement.

23. Let a_n denote the number of those permutations σ on $\{1, 2, ..., n\}$ such that σ is a product of exactly two disjoint cycles. Then:

(a) $a_5 = 50$ (b) $a_4 = 14$ (c) $a_5 = 40$ (d) $a_4 = 11$

Soln. Let a_n denote the number of those permutations σ on $\{1, 2, ..., n\}$ such that σ is a product of exactly two disjoint cycles

$$\text{No. of permutations of the type}(a)\,(bcde) = {}^5C_1 \times \frac{\lfloor 4}{4} = 30$$

$$\text{No. of permutations of the type } (ab)\,(cde) = {}^5C_2 \times \frac{\lfloor 3}{3} = 20$$

$\boxed{a_5 = 50}$.

$$\text{No. of permutations of the type } (a)\,(bcd) = {}^4C_1 \times \frac{\lfloor 3}{3} = 8$$

$$\text{No. of permutations of the type } (ab)\,(cd) = \frac{1}{2}\left({}^4C_2 \times \frac{\lfloor 2}{2}\right) = \frac{6}{2} = 3$$

$\boxed{a_4 = 11}$.

Hence, correct options are (a) and (d).

24. Find the number of elements of distinct order of S_4 ??

Soln. In S_4, $o(S_4) = 4! = 24$. There are total 24 elements.

Since 4 has 5 distinct partitions as,

$$4 = 1+1+1+1 = 1+1+2 = 1+3 = 4 = 2+2$$

Case (I)

So, corresponding to 1 + 1 + 1 + 1,

we get $\dfrac{4!}{1^4 \cdot 4!} = 1$ (element only identity)

Case (II)

Corresponding to 1 + 1 + 2,

we get $\dfrac{4!}{1^2 \cdot 2! \cdot 2^1 \cdot 1!} = \dfrac{4!}{2! \cdot 2} = 6$ elements

Case (III)

Corresponding to 1 + 3,

we get $\dfrac{4!}{1^1 \cdot 3^1 \cdot 1! \cdot 1!} = 8$ elements

Case (IV)

Corresponding to 4,

we get $\dfrac{4!}{4^1 \cdot 1!} = 6$ elements

Case (V)

Corresponding to 2 + 2,

we get $\dfrac{4!}{2^2 \cdot 2!} = \dfrac{4 \times 3 \times 2 \times 1}{2^2 \cdot 2!} = 3$ elements

and so,

total no. of elements of order 2 = 3 + 6 = 9

total no. of elements of order 3 = 8

total no. of elements of order 4 = 6

total no. of elements of order 1 = 1

25. Find the number of elements of order 2 in S_5

Partition of 5 are

(*i*) 5

(*ii*) 4 + 1

(*iii*) 3 + 2

(*iv*) 2 + 2 + 1

(*v*) 2 + 1 + 1 + 1

(*vi*) 1 + 1 + 1 + 1 + 1

Since in (*iv*) and (*v*) only l.c.m. of (2, 2, 1) and (2, 1, 1, 1) is 2. And so this cyclic decomposition show the no. of elements of order 2.

and so, corresponding to 2 + 2 + 1, we get

$$\frac{5!}{2^2 \cdot 2! \cdot 1!} = \frac{5 \times 4 \times 3 \times 2 \times 1}{2^2 \cdot 2!} = 15$$

again, corresponding to 2 + 1 + 1 + 1, we get

$$\frac{5!}{2^1 \cdot 1! \cdot (1)^3 \cdot 3!} = 10$$

Hence total 10 + 15 = 25 elements of order 2 in S_5

26. In S_5, find maximum order of an element

Soln.

$$\begin{aligned} 5 &\longrightarrow \text{L.C.M} = 5 \\ 4+1 &\longrightarrow \text{L.C.M} = 4 \\ 3+2 &\longrightarrow \text{L.C.M} = 6 \\ 2+2+1 &\longrightarrow \text{L.C.M} = 2 \\ 2+1+1+1 &\longrightarrow \text{L.C.M} = 2 \\ 1+1+1+1+1+1 &\longrightarrow \text{L.C.M} = 1 \end{aligned}$$

Hence maximum order of an element in S_5 is 6

Remarks :

We make partition into prime factors and find out in the possibility to be L.C.M. maximum

27. Find the number of elements of maximum order in S_{10}.

Soln. 10 = 2 + 3 + 5 (lcm = 30)

No. of elements of maximum order in S_{10}

$$= \frac{10!}{2 \times 3 \times 5} = 10 \times 9 \times 8 \times 7 \times 6 \times 4 = 120964$$

28. Find the number of elements of maximum order in A_{10}.

Soln. In A_{10} since there are only even permutations, so we can take only those partitions which gives us a combination of even permutation.

so, In $A_{10} = 7 + 3 \Rightarrow$ lcm = 21 be the maximum possibility to be order of an element.

And further, no. of total elements of order 21 in A_{10} is

$$\frac{10!}{3\times 7}=10\times 9\times 8\times 6\times 5\times 4\times 2=172800$$

29. Find number of element of order 2 in $S_4\times\mathbb{Z}_3$??

Soln. $S_4\times\mathbb{Z}_3$

$1 \quad 2 \quad \to 0$

$2 \quad 1 \to 9\times 1=9$

$2 \quad 2 \quad \to 0$

In case, (I) and (III) there is no possibility since $\mathbb{Z}_3$ has no element of order 2.

In case, (II), S_4 has 9 elements of order 2 and $\mathbb{Z}_3$ has 1 element of order 1 and l.c.m. (2, 1) = 2
So, total number of elements = 9 × 1 = 9 elements

30. How many subgroups of order 3 in S_4 ??

Soln. 4 = 3 + 1$\Rightarrow$ lcm = 3

$\Rightarrow\exists$ subgroups of order 3 in S_4

Number of elements of order 3 in $S_4=\dfrac{4!}{3}=8$.

so number of subgroups of order 3 in $S_4=\dfrac{8}{\phi(3)}=\dfrac{8}{2}=4$

31. If $B=(1\,2\,3)\;\;(1\,4\,5)$. Find $B^{99}=$??

Soln. $B=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&4&5\\4&5&1\end{pmatrix}$

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

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

$\Rightarrow o(B)=5\Rightarrow B^5=I$

$\therefore\;B^{5\times 20}=I\Rightarrow B^{99+1}=I$

$\Rightarrow B^{99}\cdot B=I$

$\Rightarrow B^{99}=B^{-1}$

and $B^{-1}=\begin{pmatrix}3&2&5&4&1\end{pmatrix}$

$=\begin{pmatrix}1&3&2&5&4\end{pmatrix}$ Ans.

32. The number of elements in the conjugacy class of 3-cycle (234) in the symmetric group S_6 is

(a) 20 (b) 40 (c) 120 (d) 216

Soln. The number of element in conjugacy class of (234) $=\dfrac{{}^6P_3}{3}=40=$ no. of 3 cycles

Hence, correct option is (b).

33. Let G be the group of all symmetries of the square then number of conjugate class in G are

(a) 4 (b) 5 (c) 6 (d) 7

Soln. Class equation of D_4 is 1 + 1 + 2 + 2 + 2, so number of equivalence class is 5.

Hence, correct option is (b).

34. Let σ and τ be the permutation defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 5 & 7 & 9 & 6 & 4 & 8 & 2 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 3 & 4 & 9 & 6 & 5 & 2 & 1 \end{pmatrix}. \text{ Then}$$

(a) σ and τ generates the group of permutations on {1, 2, 3, 4, 5, 6, 7, 8, 9}

(b) σ contained in the group generated by τ

(c) τ is contained in the group generated by σ

(d) σ and τ are in the same conjugacy class

35. σ and τ in cycle form are σ = (1) (2 3 5 9) (4 7) (6) (8) and τ = (1 7 5 9) (2 8) (3) (4) (6)

i.e., σ = (2 3 5 9) (4 7) and τ = (1 7 5 9) (2 8)

σ and τ have same cyclic type so they have same conjugacy class.

Hence, correct option is (d).

36. The number of conjugacy classes in the permutation group S_6 is

(a) 12 (b) 11 (c) 10 (d) 6

Soln. Conjugacy classes in the permutation group S_6 is number of partition of 6 which is 11.

Hence, correct option is (b).

37. Which of the following number can be orders of permutation σ of 11 symbols such that σ does not fix any symbol ?

(a) 18 (b) 30 (c) 15 (d) 28

Soln. $11 = 2 + 9 \rightarrow$ lcm (2, 9) = 18

$11 = 6 + 5 \rightarrow$ lcm (6, 5) = 30

$11 = 3 + 5 + 3 \rightarrow$ lcm (3, 5, 3) = 15

$11 = 4 + 7 \rightarrow$ lcm (4, 7) = 28

Hence, correct options are (a), (b), (c) and (d).

38. Let H is subgroup of S_4 and H contains (12) and (234). Then

(a) $H = A_4$ (b) $H = S_3$ (c) $H = S_4$ (d) $H = K_4$

Soln. By closure law,

$$(234)(12) = (1342) \in H$$

So $|H|$ is divisible by and 3 and 4 and |H| can be 12 or 24.

But if $|H| = 12,$ then H = $A_{4,}$ set of all even permutations but it contains odd permutation

$$\Rightarrow H \neq A_4 \Rightarrow |H| = 24 \Rightarrow H = S_4$$

Option (c) is correct

39. Let S_n denote group of permutations on n symbols then

(a) Let $H = \{\beta \in S_6 \mid \beta(1) = 1 \text{ and } \beta(4) = 4\}$ then H is not subgroup of S_6

(b) Let $H = \{\beta \in S_n \mid \beta(1) = 1 \text{ and } \beta(2) = 2\}$ Then H is subgroup of S_n for any $n \geq 3$

(c) Let $H = \{\beta \in S_n \mid \beta(1) = 1 \text{ or } 2 \text{ and } \beta(2) = 2 \text{ or } 1\}$ Then H is subgroup of S_n for any $n \geq 3$ and $|H| = 2\underline{|n-2}$

(d) None of these

Soln. For option (a)

Let $\beta, \gamma \in H$. Then $(\beta\gamma)$ (1) = $\beta(\gamma(1))$ $= \beta(1) = 1$

$(\beta\gamma)(4) = \beta(\gamma(4)) = \beta(4) = 4$

Since H is closed under group operation *G*.

$\therefore$ H is subgroup of *G*.

So option (a) is false

Also this proof is valid for $n \geq 3$

Similarly option (b) is True as H is closed under group operation. So from a subgroup.

Now for (c)

Let $\alpha, \beta \in H$, then $\alpha(1)$ is 1or 2 and $\alpha(2) = 2$ is the unused choice between 1 and 2 for $\alpha(1)$.

Similary $\beta(1)$ is 1 or 2, and $\beta(2)$ is the unused choice between 1and 2 used by $\beta(1)$. Then

$\alpha\beta(1) = \alpha(1)\, or\ \alpha\beta(1) = \alpha(2)$ and these order are 1or 2.

Same argument applies to $\alpha\beta(2)$, to find |H| observe it in matrix from we have 2 choices (1 or 2) for the image of 1, the second entry must be the choice of 1 or 2 not used as the image of 1 and $\underline{|n-2}$ choise for the remaining *n*–2 images

so $|H| = 2\underline{|n-2}$

$\therefore$ option (b) is true

Correct option are (b), (c)

40. Let *G* be a group *a*,*b*∈*G*. Then

(a) If $a^4 = 1$ and $ab = ba^2$ in a group *G*. Then *a* = 1

(b) If $a^4 = 1$ and $ab = ba^2$ in group G. Then $a \neq 1$

(c) If $a^6 = 1$ and $ab = ba^2$ in a group G, then $a^3 = 1$ and $aba = b$

(d) If $a^6 = 1$ and $ab = ba^2$ in a group G, then $a^3 = 1$ and $aba = b$

Soln. For option (a)

Since $ab = ba^2$ ....(1)

$\Rightarrow aba^2 = ba^4 = b$

Hence $a^2ba^2 = ab$ i.e. $a^2ba^2 = ba^2$ (from equation (i))

$\Rightarrow a^2 = 1$

then $ab = ba^2 = b$. $\Rightarrow a = 1$ (by cancellation law)

option (a) is correct (b) is false

For option (c)

$ab = ba^2 \Rightarrow aba^4 = ba^6 = b$

Hence $a^2ba^4 = ab = ba^2$

So, $a^2ba^2 = b$ (by cancellation law),

finally $a^3ba^2 = ab = ba^2$

So, $a^3 = 1$

Hence $\boxed{b = aba^4 = aba}$

$\therefore$ option (c) is correct and option (d) is false

Correct option are (a), (c)

41. Let S_n be the group of permutation on n symbols and $H < S_n$. Then which of the following is not true?

(a) $H = \{\alpha^2 \mid \alpha \in S_4\}$ then $H = A_4$

(b) $H = \{\alpha^2 \mid \alpha \in S_6\}$ then $H = A_6$

(c) $H = \{\alpha^2 \mid \alpha \in S_5\}$ then $H = A_5$

(d) None of these

Soln. For otption (a), Every element of H is an even permutation so $H \subseteq A_4$. Elements of A_4 has order 1,or, 2, or 3. For any α in A_4 of order 3, $\langle \alpha \rangle = \langle \alpha^2 \rangle \subset H$. The only elements in A_4 of order 2 are product of two disjoint 2-cycles s $(ab)\,(cd) = (abcd)^2 \in H \Rightarrow A_4 \subseteq H$

$\therefore\ H = A_4$

Similory for option (c), $H = A_5$.

But observe (1234) (56) = $\alpha^2 \in A_6$ but is not in H; then $|\alpha|=12$ and S_6 has no element of order 12

$\therefore H \neq A_6$

$\therefore$ option (b) is correct

PRACTICE SET-1

[Single Correct Answered Type Questions]

1. Let $H = \{I, (1\,2)\,(3\,4)\}$ and $K = \{I, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3)\}$ be subgroups of S_4, where I denotes the identity elements of S_4. Then

(a) H is cyclic but K is not abelian

(b) H is abelian but not cyclic

(c) H is cyclic and K is cyclic

(d) H is cyclic but K is non-cyclic abelian group

2. Consider the group S_9 of all the permutations on a set with 9 elements. What is the largest order of a permutation in S_9?

(a) 21 (b) 20 (c) 30 (d) 14

3. Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 3 & 2 & 1 & 8 & 7 & 5 \end{pmatrix}$. Then the order σ is

(a) 12 (b) 24 (c) 6 (d) 8

4. Which of the following statements about the permutation group on $\{1, 2, 3, \ldots\ldots, n\}$ is false ?

(a) Every element is a product of transpositions.

(b) The elements (1 2) (1 3) and (1 2) (3 4) are conjugate.

(c) Every element is a product of disjoint cycles.

(d) The group is generated by (1, 2) and $(1, 2, \ldots\ldots, n)$

5. Let $\alpha = (1\,3\,5\,7\,9\,11)$ and $\beta = (2\ 4\ 6\ 8)$ be two permutations in S_{100}, where S_{100} denotes the symmetric group on $\{1, 2, \ldots, 100\}$. Then the order of $\alpha\beta$ is

(a) 4 (b) 6 (c) 12 (d) 100

6. A permutation α of $\{1, 2, \ldots, n\}$ is called a derangement if $\alpha(i) \neq i$ for every i. Let d_n denote the number of derangements of $\{1, 2, \ldots, n)$. Then d_4 is equal to

(a) 3 (b) 9 (c) 12 (d) 24

7. Let S_3 be the group of all permutations on three symbols, with the identity element e. Then the number of elements in S_3 that satisfy the equation $x^2 = e$ is

(a) 1 (b) 2 (c) 3 (d) 4

[Multiple Correct Answer Type Questions]

1. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group and suppose it is given that g_i^2 = identity for $i = 1, 2, \ldots\ldots, n-1$. Then which is not true

(a) g_n^2 is identity and G is abelian.

(b) g_n^2 is identity but G could be non-abelian

(c) g_n^2 may not be identity

(d) None of the above can be concluded from the given data

2. Let S_n be the symmetry group of n letters and assume that it is abelian. Then choose the incorrect :

(a) $n = 1$ or $n = 2$ (b) n is a prime greater than 2

(c) n is a even number greater than 2. (d) n is a odd number greater than 2.

3. Let $(\mathbb{C} - \{0\}, \bullet)$ be the multiplicative group of all non-zero complex numbers. If G is a finite subgroups of $(\mathbb{C} - \{0\}, \bullet)$, then

(a) G is cyclic (b) G is abelian

(c) G is abelian but not cyclic (d) G is not abelian

4. For $r, s \in N$, the signature of the permutation

$$\sigma = \begin{pmatrix} 1 & 2\ldots r-1 & r & r+1\ldots r+s \\ s+1 & s+2\ldots s+r-1 & s+r & 1\ldots s \end{pmatrix} \text{ is}$$

(a) $(-1)^{rs}$ (b) $(-1)^{r+s}$ (c) $(-1)^r$ (d) $(-1)^s$

5. For a positive integer m, let $\phi(m)$, denote the number of integers k such that $1 \leq k \leq m$ and GCD $(k, m) = 1$. Then which of the following statements are necessarily true ?

(a) $\phi(n)$ divides n for every positive integer n.

(b) n divides $\phi(a^n - 1)$ for all positive integers a and n.

(c) n divides $\phi(a^n - 1)$ for all positive integers a and n such that GCD $(a, n) = 1$.

(d) a divides $\phi(a^n - 1)$ for all positive integers a and a such that GCD $(a, n) = 1$.

6. Let $\sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ be a permutation (one-to-one and onto function) such that $\sigma^{-1}(j) \leq \sigma(j)\ \forall j, 1 \leq j \leq 5$. Then which of the following are true ?

(a) $\sigma \circ \sigma(j) = j$ for all $j, 1 \le j \le 5$

(b) $\sigma^{-1}(j) = \sigma(j)$ for all $j,\ 1 \le j \le 5$

(c) The set $\{k : \sigma(k) \ne k\}$ has an even number of elements

(d) The set $\{k : \sigma(k) = k\}$ has an odd number of elements

[Numerical Answer Type Questions]

1. Let S_6 be the symmetric group of 6 symbols and $H = \left\{\sigma \in S_6 : \sigma \ne \tau\ (1\,2\,3)\ (3\,4\,6)\ \tau^{-1}, \tau \in S_6\right\}$ then cardinality of H = ??

2. The number of elements of order 5 in the symmetric groups S_5 is ??

3. Let S_{10} denote the group of permutations on ten symbols $\{1, 2, ..., 10\}$. The number of elements of S_{10} commutating with the element $\sigma = (1\ \ 3\ \ 5\ \ 7\ \ 9)$ is ??

4. The number of elements in the conjugacy class of the 3 cycle (2 3 4) in the symmetric group S_6 is ??

5. Total number of subgroups of S_3 ??

6. Maximum possible order element in S_{13} ??

7. Number of elements of order 6 in S_6 ??

SOLUTIONS OF PRACTICE TEST – 1

[Single Correct Answered Type Questions]

1. (d) since, every subgroup of prime order is always cyclic and in S_4, there is no element of order 4. So K will not be cyclic. But since it is of order $4 \Rightarrow K$ is abelian.

2. (b) 9 = 5 + 4 $\to$ lcm (5, 4) = 20.

3. (b) since, order of permutation

$= \text{l.c.m.}\ (l_1, l_2, l_3 ...)$; $\sigma = (1\,4\,3\,6)\ (2\,9\,5)\ (7\,8)$, $o(\sigma) = \text{lcm}\ \{4, 3, 2\} = 12.$

where, $l_1, l_2, ...$ are lengths of disjoint cycles.

4. (b) since, (1 2) (1 3) is a 3 cycle. But (1 2) (3 4) has {2, 2} cyclic decomposition and since in S_n conjugate elements have same cyclic decomposition. So (1 2) (1 3) and (1 2) (3 4) are not conjugate elements.

5. (c)

6. (b)

7. (d) since, three elements as (1 2), (1 3), (2 3) are of order 2 and is e itself s.t. $x^2 = e$.

[Multiple Correct Answer Type Questions]

1. Since, $g_i^2 = e \quad \forall \quad i = 1, 2, ..., n - 1$ and group is of order n. Then last element must be of order 2. Hence, group itself is abelian.
(b), (c), (d) be the Answer

2. (b), (c), (d) since S_n is non-abelian $\forall\ n \ge 3$

3. (a) and (b)

4. (a) $(-1)^{rs}$

:

inv (1) = s

inv (2) = s

$\vdots$

$\vdots$

inv $(r) = s$
inv $(r+1) = 0$

$\vdots$

$\vdots$

inv $(r+s) = 0$

And sign $\sigma = (-1)^{inv(\sigma)} = (-1)^{\sum inv(i)} = (-1)^{rs}$

5. (b), (c)

6. (a), (b), (c) and (d).

$\sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$

(i) $\sigma \circ \sigma(j) = \sigma\{1, 2, 3, 4, 5\} = \{1, 2, 3, 4, 5\} = j\ ;\ \forall j\ ; 1 \le j \le 5$

(ii) $\sigma^{-1}(j) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}\ ;\ \sigma^{-1}(j) = \sigma(j)\ ; \forall j\ ; 1 \le j \le 5$

[Numerical Answer Type Questions]

1. $H = \left\{\sigma \in S_6 : \sigma \ne \tau\,(1\,2\,3)\,(3\,4\,6)\,\tau^{-1}, \tau \in S_6\right\}.$

$$(123)(346) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4 & 6 \\ 4 & 6 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 4 & 6 & 3 \\ 2 & 4 & 6 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 6 & 3 \end{pmatrix}$$

So, number of 5-cycles in $S_6 = \dfrac{6!}{5} = \dfrac{6 \times 5 \times 4 \times 3 \times 2 \times 1}{5} = 144$

Hence, cardinality of $H = 6! - 144$ Ans

2. Elements of order 5 in symmetric group $S_5 = \dfrac{5!}{5} = 4! = 24$

3. $5 \cdot 5!$

4. 40

5. 6

6. 60

7. 240

Chapter 5

COSETS, LAGRANGES THEOREM

Coset: Suppose *G* is a group and *H* is any subgroup of *G*. Let *a* be any element of *G*. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in *G* generated by *a*. Similarly the set $aH = \{ah : h \in H\}$ is called a left coset of *H* in *G* generated by *a*.

Obviously, Ha and *aH* are both subsets of *G*. If *e* is the identity element of *G*, then $He = H = eH$. Therefore, *H* itself is a right as well as a left coset.

Since, *H* is a subgroup of *G*, therefore $e \in H$. So if *Ha* is a right coset of *H* in *G*, then *ea* is an element of *Ha*. Thus we see that $a \in Ha$. Consequently no right coset can be empty. Similarly *a* is an element of the left coset *aH*. Therefore no left coset can be empty.

If the group *G* is abelian, then we have $ah = ha \forall h \in H$. Therefore the right coset *Ha* will be equal to the corresponding left coset *aH*. However if the group G is not abelian, then we may have $aH = Ha$ or $aH \neq Ha$.

Note: If the composition in the group *G* has been denoted additively, then the right coset of *H* in *G* generated by *a* is defined as $H + a = \{h + a : h \in H\}$

Similarly, the left coset $a + H = \{a + h : h \in H\}$.

Example: Let *G* be the additive group of integers i.e. $G = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

Let *H* be the subgroup of *G* obtained on multiplying each element of *G* by 3.

Then, $H = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$. Since the group *G* is abelian then any right coset will be equal to the corresponding left coset. Let us form the right cosets of *H* in *G*.

We have $0 \in G$ and $H = H + 0 = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$.

Again, $1 \in G$ and $H + 1 = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$

Now, $2 \in G$ and $H + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$

We see that the right cosets *H*, *H*+1 and *H*+2 are all distinct and moreover these are disjoint i.e., have no element common.

Now, $3 \in G$ and $H + 3 = \{..., -6, -3, 0, 3, 6, 9, 12, ...\}$

We see that $H + 3 = H$. Also we observe that $3 \in H$.

Again, $4 \in G$ and *H* + 4 = {..., –5, –2, 1, 4, 7, 10, 13, ...}.

We see, that $H + 4 = H + 1$. Also we observe that $4 \in H + 1$.

Similarly, the right coset H + 5 coincides with *H* + 2, *H* + 6 with *H*, *H* +(–1) with *H*+2, *H*+(–2) with *H*+1 and so on. Thus we get only three distinct right cosets i.e. *H*, *H*+1, *H*+2.

Obviously, $G = H \bigcup (H + 1) \bigcup (H + 2)$.

Theorem : Let *H* is a subgroup of *G*. Then $h \in H$ iff $Hh = H = hH$

Theorem 1. If *a*, *b* are any two elements of a group G and H any subgroup of G, then

$a \in Hb \Leftrightarrow Ha = Hb$ and $a \in bH \Leftrightarrow aH = bH$.

Proof : We have,

$$a \in Hb \Rightarrow ab^{-1} \in Hbb^{-1} \Rightarrow ab^{-1} \in He$$

$\Rightarrow ab^{-1} \in H \Rightarrow Hab^{-1} = H$

$\Rightarrow Hab^{-1}b = Hb \Rightarrow Hae = Hb \Rightarrow Ha = Hb$

Conversely, let $Ha = Hb$. Since $a \in Ha$, therefore $a \in Hb$

Similarly, we can prove that $a \in bH \Leftrightarrow aH = bH$.

Theorem 2: If *H* is a subgroup of a group *G*, then *G* is equal to the union of all right cosets of *H* in *G* i.e. $G = H \bigcup Ha \bigcup Hb \bigcup Hc....$, where *a*, *b*, *c*,.... are elements of *G*.

Proof : Since *G* is a group, therefore each element of any right coset of *H* in *G* is an element of *G*. Hence the union of all right cosets of *H* in *G* is a subset of *G*.

Also, if *x* is any element of *G*, then $x \in Hx$. Therefore *x* belongs to the union of all right cosets of *H* in *G*. Hence *G* is a subset of the union of all right cosets of *H* in *G*.

Therefore, *G* is equal to the union of all right cosets of *H* in *G*. Symbolically, we have $G = \bigcup_{x \in G} Hx$.

Similarly, we can prove that *G* is also equal to the union of all left cosets of *H* in *G*.

Theorem: Two right (left) cosets are either disjoint or identical

Right coset Decomposition of a group: Suppose *H* is a subgroup of a group *G*. No right coset of *H* in *G* is empty. Any two right cosets of *H* in *G* are either disjoint or identical. The union of all right cosets of *H* in *G* is equal to *G*. Therefore the set of all right cosets of *H* in *G* gives us a partition of *G*.

This partition is called the right coset decomposition of *G* with respect to the subgroup *H*. To obtain distinct members of this partition we should proceed as follows:

First of all *H* itself is a right coset. If there is an element $a \in G$ such that $a \notin H$, then *Ha* will be another distinct right coset. Again if there is an element $b \in G$ such that $b \notin H$ and also $b \notin Ha$, then *Hb* will be another distinct right coset. Proceeding in this way we can get all distinct right cosets of *H* in *G*. Then we shall have $G = H \bigcup Ha \bigcup Hb \bigcup Hc...$, where *a*, *b*, *c*,.... are elements of *G* so chosen that all right cosets are distinct.

Similarly, we can also obtain left coset decomposition of *G*.

Theorem 3: If *H* is a subgroup of *G*, there is a one-to-one correspondence between any two right cosets of *H* in *G*.

Proof : Let $a, b \in G$. Then Ha and Hb are any two right cosets of *H* in *G*. Let $f : Ha \to Hb$ be defined by $f(ha) = hb \; \forall h \in H$.

The function *f* is one-one. If $h_1, h_2 \in H$, then $h_1a, h_2a \in Ha$. Also by def. of *f*, we have $f(h_1a) = h_1b$ and $f(h_2a) = h_2b$.

Now $f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b$

$\Rightarrow h_1 = h_2$ [by right cancellation law in *G*]

$\Rightarrow h_1a = h_2a$

Therefore, f is one-one since only equal elements of *Ha* can have the same image in *Hb*.

The function *f* is onto: Let $h'b$ be any arbitrary element of *Hb*. Then $h'b \in Hb \Rightarrow h' \in H \Rightarrow h'a \in Ha$. Now $f(h'a) = h'b,$ by definition of *f*. Thus if $h'b \in Hb \Rightarrow$ that there exists $h'a \in Ha$ such that $f(h'a) = h'b$. Therefore *f* is onto *Hb*.

Hence the result.

Similarly, it can be proved that there is a one-one correspondence between any two left cosets of *H* in *G*.

Note: *H* itself is a right as well as a left coset. Therefore if *H* is a finite subgroup of *G*, then the number of elements in *H* i.e., *o*(*H*) is equal to the number of elements in any coset of *H* in *G* (right or left).

If *H* is an infinite subgroup of *G*, then we say that any two cosets of *H* in *G* have the same Cardinal number.

Theorem 4: If *H* is a subgroup of *G*, then there is a one to one correspondence between the set of left cosets of *H* in *G* and the set of right cosets of *H* in *G*.

Note: From this theorem we conclude that if the number of distinct right cosets of *H* in *G* is finite, then it will also be equal to the number of distinct left cosets of *H* in *G*. It should be noted that in an infinite group *G*, it is possible that the number of distinct right cosets is finite.

Index of a subgroup in a group. Definition: If *H* is a subgroup of a group *G*, the number of distinct right (left) cosets of *H* in *G* is called the index of *H* in *G* and is denoted by [*G* : *H*] or by I_G (*H*).

Relation of congruence modulo a subgroup *H* in a group *G*: Suppose *H* is a subgroup of a group *G*. If the element *a* of *G* belongs to the right coset *Hb* i.e., if $a \in Hb$ i.e., if $ab^{-1} \in H$, then we say that *a* is congruent to *b* modulo *H*.

Definition: Let *H* be a subgroup of a group *G*. For $a, b \in G$ we say that *a* is congruent to *b* mod *H* if and only if, $ab^{-1} \in H$.

Symbolically, we write $a \equiv b$ (mod *H*) if and only if $ab^{-1} \in H$.

Theorem 5: The relation of congruency in a group *G* defined by $a \equiv b$ (mod *H*) *iff* $ab^{-1} \in H$ is an equivalence relation.

Illustration 1: If *G* is the additive group of integers and *H* is the subgroup of *G* obtained on multiplying the elements of *G* by 5, then we have

$G = H \bigcup (H+1) \bigcup (H+2) \bigcup (H+3) \bigcup (H+4)$. The index of *H* in *G* is 5.

2. Let *G* be the group of all permutations of degree 3 on three symbols 1, 2, 3 and *H* be the subgroup {(1), (1 2)}. The number of elements in each right coset of *H* in *G* will be 2 and the number of elements in *G* is 6. So we shall have three distinct right cosets. It can be seen that

$G = H \bigcup H(23) \bigcup H(31)$.

The left coset decomposition of *G* with respect to *H* is $G = H \bigcup (23)H \bigcup (31)H$.

Lagrange's Theorem: The order of each subgroup of a finite group is a divisor of the order of the group.

Proof : Let *G* be a group of finite order *n*. Let *H* be a sub-group of *G* and let $o(H) = m$. Suppose $h_1, h_2, ..., h_m$ are the disticnt *m* members of *H*.

Let $a \in G$. Then *Ha* is a right coset of *H* in *G* and we have

$$Ha = \{h_1 a, h_2 a, ..., h_m a\}$$

Ha has *m* distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$

Therefore, each right coset of *H* in *G* has *m* distinct members. Since *G* is a finite group, the number of distinct right cosets of *H* in *G* will be finite, say, equal to *k*. The union of these *k* distinct right cosets of *H* in *G* is equal to *G*. Thus, if $Ha_1, Ha_2, ..., Ha_k$ are the *k* distinct right cosets of *H* in *G*, then

$$G = Ha_1 \bigcup Ha_2 \bigcup ... \bigcup Ha_k$$

$\Rightarrow$ the number of elements in G = the number of elements in $Ha_1 +$ the number of elements in $Ha_2 + ... +$ the number of elements in Ha_k [$\because$ two distinct right cosets are mutually disjoint]

$\Rightarrow o(G) = km \Rightarrow n = km \Rightarrow k = \dfrac{n}{m} \Rightarrow m$ is a divisor of n

$\Rightarrow o(H)$ is a divisor of $o(G)$.

Hence the theorem

Note 1: k is the index of H in G. We have $m = n/k$. Thus k is a divisor of n.
Therefore, the index of every subgroup of a finite group is a divisor of the order of the group.

Note 2. If H is a subgroup of a finite group G, then the index of H in G = the number of distinct right (or left) cosets of H in $G = \dfrac{o(G)}{o(H)}$.

Cor. 1. The order of every element of a finite group is a divisor of the order of the group.

Proof: Suppose G is a finite group of order n. Let $a \in G$ and let $o(a) = m$. To prove that m is a divisor of n. Let $H = \{..., a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, ...\}$ be the subset of G consisting of all integral powers of a. Then we know that H is a subgroup of G. We shall show that H contains only m distinct elements and that they are $a, a^2, a^3, ..., a^m = e = a^0$.

Let $1 \le r \le m, 1 \le s \le m$ and $r > s$.

Let $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \Rightarrow a^{r-s} = a^0 \Rightarrow a^{r-s} = e$

Thus, there exists a positive integer $r - s$ less than m such that $a^{r-s} = e$. But m is the least positive integer such that $a^m = e$. Therefore $a^r \ne a^s$. Therefore $a, a^2, a^3, ..., a^m = a^0 = e$ are all distinct elements of H. Now suppose a^t is any element of H, where t is any integer. By division algorithm, we have $t = mp + q$ where p and q are some integers and $0 \le q < m$.

[Note: We can write $t/m = p + q/m$]

We have,

$a^t = a^{mp+q} = a^{mp}a^q = (a^m)^p a^q = ea^q = a^q$. Since $0 \le q < m$,

therefore, a^q is one of the m elements $a, a^2, ..., a^m = a^0$. Hence H has only m distinct element.

Thus, order of H is m. By Lagrange's theorem m is a divisor of n.

Cor.2. If G is a finite group of order n and $a \in G$, then $a^n = e$.

Proof : In a finite group, the order of each element is finite. Let $o(a) = m$. The subset H of G consisting of all integral powers of a is a subgroup of G and the order of H is m. By Lagrange's theorem m is a divisor of n. Let $k = \dfrac{n}{m}$. Then $n = mk$.

Now $a^n = a^{mk} = (a^m)^k = e^k$ [$\because o(a) = m \Rightarrow a^m = e$] $= e$

Note: Lagrange's theorem has very important applications. Suppose G is a finite group of order n. If m is not a divisor of n, then there can be no subgroup of G of order m. Thus if G is a group of order 6, then there can be no subgroup of G of order 5 and 4. Similarly if G is a group of prime order p, then G can have no proper subgroups.

However, the converse of Lagrange's theorem is not true.

If m is a divisor of n, then it is not necessary that G must have a subgroup of order m.

For example, the alternating group A_4 is of order 12. It can be seen that there is no sub-group of A_4 of order 6, though 6 is a divisor of 12.

Cor.3. Euler's Theorem: If n is a positive integer and a is any integer relatively prime to n, then $a^{\phi(n)} \equiv 1(\text{mod}\, n)$, where ϕ is the Euler ϕ-function.

Proof: For any integer x, let $[x]$ denote the residue class of the set of integers mod n. Let $G = \{[a] : a$ is an integer relatively prime to $n\}$.

Then we know that with respect to multiplication of residue classes G is a group of order $\phi(n)$. The identity element of this group is the residue class [1]. We have

$[a] \in G \Rightarrow [a]^{o(G)} = [1] \Rightarrow [a]^{\phi(n)} = [1]$

$\Rightarrow [a][a][a]...$ upto $\phi(n)$ times = [1]

$\Rightarrow [aa...$ upto $\phi(n)$ times] = [1] [Note that $[a]$ $[b]$ = $[ab]$]

$\Rightarrow [a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} \equiv 1(\text{mod}\, n)$

Cor.4. Fermat's theorem: If p is a prime number and a is any integer, then $a^p \equiv a(\text{mod}\ p)$.

Proof: Let G be the set of non-zero residue classes of integers modulo p. If p is a prime number, then with respect to multiplication of residue classes G is a group of order p–1. The identity element of this group is [1].

Now suppose a is any integer.

Case 1. p is a divisor of a. In this case $[a] = [0]$ and so $[a]$ is not an element of G. But

$p \,|\, a \Rightarrow p \,|\, a^p \Rightarrow p \,|\, (a^p - a) \Rightarrow a^p \equiv a(\text{mod}\ p)$

Case 2. p is not a divisor of a. In this case $[a] \neq [0]$ and so $[a]$ is an element of G. Therefore we have

$[a]^{o(G)} = [1] \Rightarrow [a]^{p-1} = [1] \Rightarrow [a^{p-1}] = [1] \Rightarrow a^{p-1} \equiv 1(\text{mod}\ p)$

$\Rightarrow a^{p-1} - 1$ is divisible by $p \Rightarrow a(a^{p-1} - 1)$ is divisible by p

$\Rightarrow a^p - a$ is divisible by $p \Rightarrow a^p \equiv a(\text{mod}\ p)$.

Order of the product of two subgroups of finite order.

Theorem 6: Let H and K be finite subgroups of a group G. Then $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}$.

Corollary: Let H and K be subgroups of a finite group G and let $o(H) > \sqrt{[o(G)]}, o(K) > \sqrt{[o(G)]}$. Then $H \cap K \neq \{e\}$.

Proof: Since, $HK \subseteq G$, therefore $o(HK) \leq o(G)$ ...(1)

But, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}$ ...(2)

From (1) and (2), we get $o(G) \geq \dfrac{o(H)o(K)}{o(H \cap K)}$ ...(3)

But, $\dfrac{o(H)o(K)}{o(H\bigcap K)} > \dfrac{\sqrt{[o(G)]}\sqrt{[o(G)]}}{o(H\bigcap K)}$ [by hypothesis]

i.e., $\dfrac{o(H)o(K)}{o(H\bigcap K)} > \dfrac{o(G)}{o(H\bigcap K)}$ ...(4)

From (3) and (4), we get $o(G) > \dfrac{o(G)}{o(H\bigcap K)}$

Therefore, $o(H\bigcap K) > 1$ and this implies that $H\bigcap K \neq \{e\}$ because order of $\{e\} = 1$.
We apply this corollary to a very special group.

Example: Let *G* be a finite group of order *pq* where *p* and *q* are prime numbers with *p*>*q*. Then G has at most one subgroup of order *p*. In particular a group of order 6 has at most one subgroup of order 3.

Soln. If possible, let *H* and *K* be the two subgroups of *G* of the same order *p*. Since *p* > *q* and $o(G) = pq$, therefore $o(H) > \sqrt{[o(G)]}$ and $o(K) > \sqrt{[o(G)]}$. So by the above corollary $H\bigcap K \neq \{e\}$.

Now, $H\bigcap K$ is a subgroup of *H*. Since *H* is of prime order *p*, therefore either $H\bigcap K = H$ or $H\bigcap K = \{e\}$. But $H\bigcap K \neq \{e\}$. Therefore $H\bigcap K = H$ and this implies that $H \subseteq K$. Similarly we can prove that $K \subseteq H$. Hence $H = K$. Therefore there can be at most one subgroup of *G* of order *p*. As a special case of group of order six has at most one subgroup of order 3 since 6 = 3×2 where 3>2 and both 3 and 2 are primes.

Normal Subgroups : A subgroup *H* of a group *G* is normal if $gH = Hg\ \forall\ g \in G$.

e.g., $H = \{1,-1\}$ is a normal subgroup of the Quaternion group *G*. Indeed $Ha = \{a,-a\} = aH$ for any $a \in G$.

Theorem-1 : A subgroup *H* of a group *G* is normal in *G* iff $g^{-1}Hg = H$ for all $g \in G$.

Proof : Let *H* be normal in *G* then $Hg = gH$ for all $g \in G$.

$\Rightarrow g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)H = H$

Conversely, let $g^{-1}Hg = H$ for all $g \in G$, then $g(g^{-1}Hg) = gH$

$\Rightarrow (gg^{-1})Hg = gH \Rightarrow Hg = gH$

Hence, *H* is normal.

Theorem-2 : A subgroup *H* of a group *G* is normal in *G* iff $g^{-1}Hg \subseteq H$ for all $h \in H, g \in G$.

Theorem-3 : A subgroup *H* of a group *G* is normal subgroup of *G* iff product of two right cosets of *H* in *G* is again a right coset of *H* in *G*.

Results and properties of Normal subgroups:

1. Every subgroup *H* of a group *G* of index 2 is always normal in *G*.

2. If a cyclic subgroup *K* of *G* is normal in *G* then every subgroup of *K* is normal in *G*.

3. *Z*(*G*) is always normal in *G*.

4. If *H* and *K* are two normal subgroups of a group *G* such that $H \cap K = \{e\}$ then show that $hk = kh$ for all $h \in H, k \in K$.

Quotient group or Factor group : Let *G* be a group and *N* be a normal subgroup of *G*. Let us collect all the right cosets of *N* in *G* and form a set to be denoted by *G*/*N*. Since *N* is normal in *G*, product of any two right cosets of *N* will again be a right coset of *N* in *G*.

Theorem-1 : If G is a finite group and N is a normal subgroup of G then $o\left(\frac{G}{N}\right)=\frac{o(G)}{o(N)}$.

Proof : Since G is finite, using Lagrange's theorem $\frac{o(G)}{o(N)}=$ number of distinct right cosets of N in $G=o\left(\frac{G}{N}\right)$.

Theorem-2 : Every quotient group of a cyclic group is cyclic.

Result and property

1. If G is a group such that $G/Z(G)$ is cyclic then G is abelian where $Z(G)$ is centre of G.

Solved Examples

1. Let G be a group of order 30. Let A and B be normal subgroups of order 2 and 5 respectively, then order of the group G/AB is

(a) 10 (b) 3 (c) 2 (d) 5

Soln. $A \triangleleft G, B \triangleleft G, o(A)=2, o(B)=5$

$$o(AB)=\frac{o(A)\cdot o(B)}{o(A\cap B)}$$

2 and 5 are prime, so A and B are cyclic, $\mathrm{A}\approx\mathbb{Z}_2,\ \mathrm{B}=\mathbb{Z}_5$

As $\gcd(2,5)=1$, so $o(A\cap B)=1 \Rightarrow o(AB)=10$

So $o\left(\frac{G}{AB}\right)=\frac{o(G)}{o(AB)}=\frac{30}{10}=3.$

Hence, correct option is (b).

2. Every subgroup of order 74 in a group of order 148 is normal. True or False ? **[TIFR-2012]**

Ans. True

Soln. Every subgroup of index 2 is normal in G.
Hence it is normal in G.

3. How many normal subgroups does a non-abelian group G of order 21 have other than the identity subgroup $\{e\}$ and G ?

(a) 0 (b) 1 (c) 3 (d) 7

Soln. $o(G)=21;\ pq=3\times 7;\ p|(q-1)=3|(7-1)$

Hence, only 'one' normal subgroup does a non-abelian group G of order 21 have other than the identity subgroup $\{e\}$ and G .

Hence, correct option is (b).

4. The converse of Lagrange's theorem does not hold in

(a) A_4, the alternating group of degree 4 (b) $A_4 \times \mathbb{Z}_2$

(c) the additive group of integers modulo 4 (d) Klein's four group **[D.U. 2014]**

Soln. In A_4, there is no subgroup of order 6 but 6|12.

Hence, correct option is (a).

5. Let G be a group of order 45. Let H be a 3-sylow subgroup of G and K be a 5-sylow subgroup of G. Then,

(a) both H and K are normal in G (b) H is normal in G but K is natural in G

(c) H is not normal in G but K is normal in G (d) both H and K are not normal in G

Soln. $|G| = 45 = 3^2 \cdot 5$. From (question-1), $n_5 = 1 \Rightarrow$ it has unique 5-sylow subgroup by sylow 2nd theorem it is normal in G. By $n_3 = 1 \Rightarrow$ 3-sylow subgroup is normal.

Hence, correct option is (a).

6. Upto isomorphism the number of abelian group of order 10^5 is

(a) 2 (b) 5 (c) 7 (d) 49

Soln. $|a| = 2^5 5^5$

The number of abelian group of order 10^5 upto isomorphism =

$P(5) \cdot P(5) = 7 \cdot 7 = 49$ where $P(5) =$ partition of 5.

Hence, correct option is (d).

7. The number of non-isomorphic groups of order 10 is_____.

Ans. 2

Soln. Let G be a group of order 10. $|G| = 10 = 2 \times 5$, $G \approx D_5$ or $\mathbb{Z}_{10}$

8. The number of non-isomorphic abelian group of order 24 is_____.

Ans. 3

Soln. $|G| = 24 = 2^3 3$

Number of non-isomorphic abelian group $= P(3)P(1) = 3$, where $P(n)$ is a partition of n.

9. Up to isomorphism, the number of abelian groups of order 108 is

(a) 12 (b) 9 (c) 6 (d) 5

Soln. If $o(G) = p^a q^b r^c$ then number of abelian group upto isomorphism is $P(a) \cdot P(b) \cdot P(c)$....., where $P(n)$ = partition of n.

$o(G) = 108 = 2^2 \times 3^3$

Number of abelian group = 6. i.e., $P(2) \cdot P(3) = 6$ where $P(n)$ = partition of n.

Hence, correct option is (c).

10. Consider a group G. Let $Z(G)$ be its centre, i.e., $Z(G) = \{g \in G : gh = hg$ for all $h \in G\}$ for $n \in \mathbb{N}$ the set of positive integers define $J_n = \{(g_1, ..., g_n) \in Z(G) \times ... \times Z(G) \mid g_1 ... g_n = e\}$, As a subset of the direct product group $G \times G \times ... \times G$ (n times direct product of the group G), J_n is

(a) not necessarily a subgroup

(b) A subgroup but not necessarily a normal subgroup

(c) A normal subgroup

(d) Isomorphic to the direct product $Z(G) \times ... \times Z(G)$ $(n-1)$ times

Soln. Given that, $J_n = \{(g_1, ..., g_n) \in Z(G) \times ... \times Z(G) \mid g_1 ... g_n = e\}$ which is center of G and we know that $Z(G)$ is always normal in G

Hence, correct option is (c).

11. For any group G of order 36 and any subgroup H of order 4

(a) $H \subset Z(G)$ (b) $H = Z(G)$ (c) H is normal in G (d) H is an abelian group

Soln. Every group of order p^2 is always abelian and every sub group of abelian group is abelian.
Hence, correct option is (d).

12. S_n = symmetric group of permutations of n-symbols
A_n = set of all even permutation on n-symbols then
(a) A_n is subgroup of S_n and but not a normal subgroup of S_n
(b) A_n is normal subgroup of S_n and S_n/A_n is cyclic
(c) A_n is normal subgroup of S_n but S_n/A_n is not cyclic
(d) A_n is not a subgroup of S_n

Soln. A_n is normal subgroup of S_n because index of A_n is 2 in S_n and $\frac{S_n}{A_n} \cong \mathbb{Z}_2 \Rightarrow$ cyclic

Hence, correct option is (b).

13. Show that two right cosets Ha, Hb are distinct if and only if the two left cosets $a^{-1}H, b^{-1}H$ are distinct.

Soln. In order to prove the given statement we shall prove that two right cosets Ha, Hb are equal if and only if the two left cosets $a^{-1}H, b^{-1}H$ are equal. We have

$$Ha = Hb \Leftrightarrow ab^{-1} \in H$$

$$\Leftrightarrow ab^{-1}H = H \qquad [\because h \in H \Leftrightarrow hH = H]$$

$$\Leftrightarrow a^{-1}ab^{-1}H = a^{-1}H \Leftrightarrow b^{-1}H = a^{-1}H \Leftrightarrow a^{-1}H = b^{-1}H$$

Hence the required result follows.

14. Show that the set of the inverse of the elements of a right coset is a left coset; or more precisely show that $(Ha)^{-1} = a^{-1}H$.

Soln. Suppose Ha is a right coset of H in G where $a \in G$.
Let ha be any element of Ha, where $h \in H$.
We have,

$$(ha)^{-1} = a^{-1}h^{-1}$$

Since, H is a subgroup, therefore $h \in H \Rightarrow h^{-1} \in H$

$\therefore a^{-1}h^{-1} \in a^{-1}H$

Thus, the inverses of all the elements of Ha belong to the left coset $a^{-1}H$. Hence $(Ha)^{-1} \subseteq a^{-1}H$

Conversely, let $a^{-1}h$ be any element of $a^{-1}H$.

Then $a^{-1}h = a^{-1}(h^{-1})^{-1} = (h^{-1}a)^{-1} \in (Ha)^{-1}$, since $h^{-1} \in H$ and therefore $h^{-1}a \in Ha$.

Therefore, every element of $a^{-1}H$ belongs to the set of the inverses of the elements of Ha.

$\therefore\ a^{-1}H \subseteq (Ha)^{-1}$

Hence, $(Ha)^{-1} = a^{-1}H$.

15. Given that $G = H \bigcup Ha_2 \bigcup Ha_3 ... \bigcup Ha_k$ is the right coset decomposition of G relative to the subgroup H, show that $G = H \cup a_2{}^{-1}H \cup a_3{}^{-1}H \cup .... \cup a_k{}^{-1}H$ is a left coset decomposition of G relative to the subgroup H.

Soln. We know that two right cosets of H in G are either disjoint or identical. Therefore if there are two equal right cosets in the given right coset decomposition of G, then one of them can be omitted. So let us assume that all the right cosets in the given right coset decomposition of *G* relative to *H* are distinct. Then there are *k* distinct right cosets of *H* in *G*. But the number of distinct right cosets of *H* in *G* is equal to the number of distinct left cosets of *H* in *G*. Therefore there are *k* distinct left cosets in the left cosets decomposition of *G* relative to *H*.

Now we know that two right cosets *Ha* and *Hb* are distinct if and only if the two left cosets $a^{-1}H$ and $b^{-1}H$ are distinct. Since the right cosets $H, Ha_2, ..., Ha_k$ are all distinct, therefore the left cosets $H, a_2^{-1}H, ..., a_k^{-1}H$ are all distinct. Since they are *k* in number, therefore they are the only distinct left cosets of *H* in *G*. Now the union of all the distinct left cosets of *H* in *G* is equal to *G*. Hence

$$G = H \bigcup a_2^{-1}H \bigcup a_3^{-1}H \bigcup ... \bigcup a_k^{-1}H$$

is a left coset decomposition of *G* relative to the subgroup *H*

16. Prove that the only right (or left) coset of a subgroup *H* in a group *G* which is also a subgroup of *G* is *H* itself.

Soln. Suppose *Ha* is a right coset of *H* in *G*. Let *Ha* be a subgroup of *G*. Then $e \in Ha$. But $e \in H$. Since, *H* is itself a right coset and two cosets are either disjoint or identical, therefore *H* = *Ha*.

Similarly, *aH* is a subgroup of $G \Rightarrow aH = H$.

17. If $H \subseteq K$ are two subgroups of a finite group *G*, then show that $[G:H] = [G:K][K:H]$.

Soln. Since, $H \subseteq K$ are two subgroups of a group *G*, therefore *H* is also a subgroup of *K*.
Now, *H* is a subgroup of a finite group *G*. Therefore by Lagrange's theorem

$$[G:H] = \frac{o(G)}{o(H)} = \frac{o(G)}{o(K)} \cdot \frac{o(K)}{o(H)} = [G:K]\,[K:H]$$

18. Let *H* and *K* be two subgroups of a group *G*. Show that any coset relative to $H \bigcap K$ is the intersection of a coset relative to *H* with a coset relative to *K*.

Soln: Let *a* be any element of *G*. Then $(H \bigcap K)\,a$ is any right coset of *G* relative to the subgroup $H \bigcap K$. We shall prove that $(H \bigcap K)a = (Ha) \bigcap (Ka)$

We have,

$$(H \bigcap K) \subseteq H \Rightarrow (H \bigcap K)a \subseteq Ha$$

and $(H \bigcap K) \subseteq K \Rightarrow (H \bigcap K)a \subseteq Ka$

$\therefore (H \bigcap K)a \subseteq Ha \bigcap Ka$

Again, let *x* be any element of $Ha \bigcap Ka$. Then $x \in Ha$ and $x \in Ka$

$\therefore x = ha = ka$ for some $h \in H$, $k \in K$

$\therefore xa^{-1} = h = k$

$\therefore xa^{-1} \in H \bigcap K \Rightarrow (xa^{-1})a \in (H \bigcap K)a \Rightarrow x \in (H \bigcap K)a$

Consequently, $Ha \bigcap Ka \subseteq (H \bigcap K)a$.

From (1) and (2), we conclude that $(H \bigcap K)a = Ha \bigcap Ka$
A similar proof can be given in the case of a left coset.

19. Prove that the intersection of two subgroups, each of finite index, is again of finite index.

Soln. Let *H* and *K* be two subgroups of a group *G*. Let $[G:H] = m$ and $[G:K] = n$. Let $Ha_1, ..., Ha_m$ and $Kb_1, ..., Kb_n$ be the distinct right cosets of *H* and *K* respectively. We are to show that the number of distinct right cosets of $H \bigcap K$ in *G* is finite. Let $(H \bigcap K)\,a$ be any right coset of $H \bigcap K$ in *G*. Then it can be easily shown that $(H \bigcap K)a = Ha \bigcap Ka$. Thus each right coset of $H \bigcap K$ is given by the intersection of a right cosets of H and a right coset of *K*. Since the number of distinct right cosets of *H* in *m* and the number of distinct right cosets of *K* is *n*, therefore the number of distinct right cosets of $H \bigcap K$ can be at most equal to *mn*. Hence $H \bigcap K$ is of finite index in *G*.

20. Use Lagrange's theorem to prove that a finite group cannot be expressed as the union of two of its proper subgroups.

Soln. Let *G* be a finite group of order *n*. Suppose *G* is the union of two of its proper subgroups *H* and *K*. Since, $e \in$ both *H* and *K* and $G = H \bigcup K$, therefore at least one of *H* and *K* (say, *H*) must contain more than half the elements of *G*. Let $o(H) = p$. Then $n/2 < p < n$. (Note that *H* is a proper subgroup of *G*). Since, $n/2 < p < n$, therefore *p* cannot be a divisor of *n*. This contradicts Lagrange's theorem which states that the order of each subgroup of a finite group is a divisor of the order of the group.
Hence our initial assumption is wrong and so a finite group cannot be expressed as the union of two of its proper subgroups.

21. Let G be a finite group and let N be a normal subgroup of G. Suppose order of *N* is n relatively prime to the index $|G:N| = m$. Then

(a) $N = \{a \in G \mid a^n = e\}$ (b) $N = \{b^m \mid b \in G\}$

(c) $N = \{a \in G \mid a^m = e\}$ (d) $N = \{a^n \mid a \in G\}$

Soln. Note that as n and m are relatively prime integers $\exists\, s, t \in \mathbb{Z}$ such that

sn + tn = 1 ...(i)

Also $\left|\frac{G}{N}\right| = |G:N| = m$, we have $g^m N = (gN)^m = N$ for any

$g \in G$ by Lagrange's theorem $g^m \in N$ ...(ii)

For option (a)

Supper $a \in \{a \in G \mid a^n = e\}$. Then we have $a^n = e$

$$\Rightarrow a = a^{sn+tm} = a^{sn}a^{tm} = a^{tm} = (a^t)^m \in N$$

$$\Rightarrow \{a \in G; a^n = e\} \subset N$$

If $a \in N$, then $a^n = e$ as n is order of group N.

Hence $N \subseteq \{a \in G \mid a^n = e\}$

$$\therefore\ N = \{a \in G \mid a^n = e\}$$

option (a) is corret and (c) is false

For option (b)

Let $b^m \in \{b^m \mid b \in G\}$. then by (ii), we know that $b^m \in N$

Thus, we have $\{a^m \mid b \in G\} \subseteq N$

Now, if $a \in N \Rightarrow a^n = e$ as $n = |N|$

If follows that $a = a^{sn+tm} = a^{sn}a^{tm} = b^m$ (Where we put $b = a^t$)

$\Rightarrow a \in \{b^m \mid b \in G\}$ and $N \subseteq \{b^m + b \in G\}$

$\therefore\ N = \{b^m ; b \in G\}$

Option (b) is correct and (d) is false

Correct option (a) and (b)

22. Let $G = GL(2, R)$ be the group with non zero deteminant .Let H be the subgroup of matrices of determinant ± 1. If $a,b, \in G$ and $aH = bH$, then

(a) det a = det b

(b) det (a) = –1, det (b) = 1

(c) det (a) = 1, det (b) = –1

(d) None of these

Soln. If $aH = bH \Rightarrow b^{-1}a \in H$

So, $\det(b^{-1}a) = \det(b^{-1})\det(a)$

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

thus det a = det b

Converesly, let $\det a = \det b$

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

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

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

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

$\Rightarrow aH = bH$

$\therefore$ option (a) is true and (b) (c) are false

Correct option is (a)

23. Let H be a subgroup of S_n such that H contain an odd permutation, then

(a) $\exists$ a subgroup M of H with index 2 in H

(b) $\nexists$ a subgroup M of H with index 2 in H

(c) HA_n need not be isomorphic to S_n

(d) None of these

Soln. Since $A_n \Delta S_n$ and H is subgroup of $S_n, K = HA_n$ will be a subgroup of S_n.

Also $A_n \subseteq K \subseteq S_n \Rightarrow$ either $K = S_n$ *or* $K = A_n$

Also, $H \subseteq HA_n = K$ and H has an odd permutation, K has an odd permutation and so $K \neq A_n$

Hence K = S_n

Now, $\frac{HAn}{A_n} \cong \frac{H}{H \cap A_n}$ (second theorem of isomorpism)

and as $HA_n = K = S_n$

We have $\frac{S_n}{A_n} \cong \frac{H}{H \cap A_n} \Rightarrow o\left(\frac{H}{H \cap A_n}\right) = o\left(\frac{S_n}{A_n}\right) = 2$

Take $M = H \bigcap A_n$ then index of M in H is 2

then option (b),(c) are false

Correct option is (a)

24. Let S_4 be symmetric group on four symbol's and $H = \{\sigma \in S_4 : 0(\sigma) = \text{odd number}\}$ be a subset of $S_{4,}$. Thenwhich of the following is true ?

(a) H is subgroup of A_4

(b) H is subgroup of S_4 but not subgroup of A_4

(c) $H \bigcap (S_4 \setminus A_4)$ is non empty

(d) $H \bigcap (S_4 \setminus A_4)$ is empty

Soln. take $\sigma = (134) \in H$ and $\tau = (124) \in H$

$o(\sigma) = 0(\tau) = 3$

But $(\sigma\tau) = (134)(124) = ((12)(34))$

$\Rightarrow o(\sigma\tau) = 2$ = even number

$\Rightarrow (\sigma\tau) \notin H$

H is not a subgroup of S_4 and also it is subgroup of A_4

$\therefore$ option (a), (b) are false

If $\sigma \in H$ then s is either odd length cycle or product of disjoint odd length cycle

$\Rightarrow \sigma$ is even permutation

$\Rightarrow H \subseteq A_n (\forall n \geq 3)$

$\Rightarrow H \bigcap (S_n \setminus A_n) = \text{empty}$

Option (d) is correct and option (c) is false

Correct option is (d)

Properties of Cosets:

Let H be a subgroup of G and let $a,b \in G$. Then,

1. $a \in aH$

2. $aH = H$ if and only if $a \in H$

3. $aH = bH$ or $aH \bigcap bH = \phi$ i.e. any two left (right) cosets of H are either disjoint or identical.

4. $aH = bH$ if and only if $a^{-1}b \in H$

5. $|aH| = |bH|$

6. $aH = Ha$ if and only if $H = aHa^{-1}$

7. aH is a subgroup of G if and only if $a \in H$

Proof:

1. $a = ae \in aH$

2. To verify property 2, we first suppose that $aH = H$. Then $a = ae \in aH = H$. Next we assume that $a \in H$ and show that $aH \subseteq H$ and $H \subseteq aH$. The first inclusion follows directly from the closure of *H*. To show that $H \subseteq aH$, let $h \in H$. Then, since $a \in H$ and $h \in H$, we know that $a^{-1}h \in H$. Thus, $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$

3. To prove property 3, we suppose that $aH \cap bH \neq \phi$ and prove that $aH = bH$. Let $x \in aH \cap bH$. Then there exist h_1, h_2 in *H* such that $x = ah_1$ and $x = bh_2$. Thus, $a = bh_2h_1^{-1}$ and $aH = bh_2h_1^{-1}H = bH$, by property 2.

4. Observe that $aH = bH$ if and only if $H = a^{-1}bH$. The result now follows from property 2.

5. We leave it as an exercise for the student to prove that the correspondence $ah \to bh$ for all *h* in H is a one-to-one, onto function from *aH* to *bH*.

6. Note that $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1}$ that is, if and only if $aHa^{-1} = H$.

7. If *aH* is a subgroup, then it contains the identity *e*. Thus, $aH \cap eH \neq \phi$; and, by property 3, we have $aH = eH = H$. Thus, from property 2, we have $a \in H$. Conversely, if $a \in H$, then, again by property 2, $aH = H$.

Chapter 6

NORMAL SUBGROUP

Normal Subgroup:

Let *G* be a group under multiplication and *H* be any subgroup of *G* and let $x \in G$. Then Hx and xH are respectively the right and left cosets of *H* in *G*.

If *G* is abelian then $Hx = xH \ \forall x \in G$.

But even when *G* is non abelian and yet there exist a subgroup *H* of *G* having the property $Hx = xH \ \forall x \in G$, then such a subgroup of *G* is called normal subgroup.

A normal subgroup *H* of a group *G* is denoted by $H \triangleright G$

Definition: A subgroup *H* of *G* is called normal subgroup of *G* if $xhx^{-1} \in H$ for all $x \in G$ and for all $h \in H$.

Note: For a group *G*, $\{e\}$ and *G* are always the normal subgroups of *G* and these are called trivial normal subgroups of *G* or improper normal subgroups of *G*.

Simple Group: If a group *G* has no proper normal subgroup, then *G* is called a simple group

Note: Every group of prime order is simple.

Theorem 1: Every subgroup of an abelian group is always normal

Theorem 2: A subgroup *H* of a group *G* is normal if and only if $xHx^{-1} = H$ for all $x \in G$

Theorem 3: A subgroup *H* of a group *G* is normal if and only if each left coset of *H* in *G* is a right coset of *H* in *G*.

Theorem 4: A subgroup *H* of *G* is normal if and only if the product of two right cosets of *H* in *G* is again a right cosets of *H* in *G*.

Theorem5: Intersection of two normal subgroups of a group is also a normal subgroup

Theorem6: Intersection of any collection of normal subgroups is itself a normal subgroup

Theorem7: If *M* and *N* are two normal subgroups of *G* such that, $N \bigcap M = \{e\}$, then for every $n \in N$ and $m \in N$ we have *nm*= *mn*.

Theorem 8: Let *H* be a subgroup of *G* and *N* be a normal subgroup of *G*. Then $H \cap N$ is a subgroup of *H*.

Solved Examples

1. If H is a subgroup of G and N is a normal subgroup of G, then $H \cap N$ is a normal subgroup of

(a) H (b) N (c) $H+N$ (d) G **[B.H.U.-2011]**

Soln. Let $x \in H \bigcap N$

$\Rightarrow x \in H$ and $x \in N$

Let $h \in H \Rightarrow h \in G$

$\Rightarrow hxh^{-1} \in H$ ($\because$ H is subgroup of G)

Also $hxh^{-1} \in N$ ($\because$ N is normal subgroup of G)

$\Rightarrow hxh^{-1} \in H \bigcap N \ \forall h \in H, \forall x \in H \bigcap N$

$H \bigcap N$ is normal subgroup of H.

Hence correct option is (a)

2. Let H be a finite subgroup of a group G and let $g \in G$. If $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$, then **[B.H.U-2018]**

(a) $\left|gHg^{-1}\right| = |H|$ (b) $\left|gHg^{-1}\right| < |H|$

(c) $\left|gHg^{-1}\right| > |H|$ (d) $\left|gHg^{-1}\right| = 1$

Soln. Define $f : H \to gHg^{-1}$ by $f(h) = ghg^{-1}, h \in H$

Let $h_1, h_2 \in H$

$f(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = f(h_1)f(h_2)$

$\Rightarrow f$ is a homomorphism

Let $f(h_1) = f(h_2)$

$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$

$\Rightarrow h_1 = h_2$

$\Rightarrow f$ is one- one

Let $x \in gHg^{-1}$

$\Rightarrow \ x = gh_1g^{-1}$ for some $h_1 \in H$

Now $h_1 \in H$

$\Rightarrow f\ (h_1) = gh_1g^{-1}$

$\Rightarrow f$ is onto

$\Rightarrow f$ is one-one and onto

$\Rightarrow \left|gHg^{-1}\right| = |H|$

Hence correct option is (a)

3. Let G be a finite group and H is a subgroup of G of index 2. Then **[H.C.U. 2018]**

(a) H is normal and $g^2 \in H$ for any $g \in G$ (b) H is normal and $g^2 = e$

(c) H is need not be normal (d) None of the above

Soln. Given H is a subgroup of G of index 2

$\Rightarrow$ H is normal in G and also $(gH)^2 = H \ \forall g \in G$ (it is normal because every right coset is also a left coset)

$\Rightarrow (gH)(gH) = H$

$\Rightarrow g^2H = H$ ($\because$ H is normal in G)

$\Rightarrow g^2 \in H$ ($\because h \in H \Leftrightarrow Hh = H = hH$)

Hence correct option is (a)

4. Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Q} - \{0\}, b \in \mathbb{Q} \right\}, U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Q} \right\}, \ D = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Q} - \{0\} \right\}$

Which of the following statements are true? **[H.C.U. 2013]**

(a) G, U, D are all groups under multiplication (b) D is a normal subgroup of G

(c) U is a normal subgroup of G (d) For every matrix $A \in U$, $ADA^{-1} \subseteq D$

Soln. Given $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Q} - \{0\}, b \in \mathbb{Q} \right\}$

$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Q} \right\}, D = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Q} - \{0\} \right\}$

We can easily prove that G, U,D are all groups under multiplication.

Also $U \subseteq G$ and $D \subseteq G$

$\Rightarrow U$ and D are subgroups of G.

To check that D is normal in G or not :

Let $B \in G$ and $C \in D$

$\Rightarrow B = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}$ for some $a_1 \in \mathbb{Q} - \{0\}, b_1 \in \mathbb{Q}$ and $C = \begin{pmatrix} a_3 & 0 \\ 0 & 1 \end{pmatrix}$ for some $a_3 \in \mathbb{Q} - \{0\}$

Now $BCB^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a_1} & \frac{-b_1}{a_1} \\ 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{a_3}{a_1} & \frac{-a_3 b_1}{a_1} \\ 0 & 1 \end{pmatrix}$

$$=\begin{pmatrix} a_3 & -a_3b_1+b_1 \\ 0 & 1 \end{pmatrix} \notin D$$

$\Rightarrow D$ is not normal in G.

To check that U is normal in G or not

Let $B \in G$ and $C \in U$

$$\Rightarrow \; B=\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \text{ for some } a_1 \in \mathbb{Q}-\{0\}, b_1 \in \mathbb{Q} \text{ and } C=\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}; b_2 \in \mathbb{Q}$$

$$BCB^{-1}=\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a_1} & -\frac{b_1}{a_1} \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a_1} & \frac{-b_1}{a_1}+b_2 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & -b_1+a_1b_2+b_1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & a_1b_2 \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow BCB^{-1} \in U$

$\Rightarrow U$ is normal in G.

Let $A \in U$

$$\Rightarrow A=\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}; b \in \mathbb{Q}$$

Now $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & -ab \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & -ab+b \\ 0 & 1 \end{pmatrix} \notin D$

$\Rightarrow ADA^{-1} \not\subseteq D$

Correct option is (a) and (c)

5. For a group G, which of the following statements are true? **[H.C.U. 2014]**

(a) If $x, y \in G$ such that order of x is 3, order of y is 2 then order of xy is 6.

(b) If every element is of finite order in G then G is a finite group

(c) If all subgroups are normal in G then G is abelian

(d) If G is abelian then all subgroups of G are normal

Soln. For option (a)

Take $G=S_3$

Let $x=(123)$ and $y=(12)$

Clearly $o(x)=3$ and $o(y)=2$

$xy=(123)(12)=(1)(23)$

$\Rightarrow o(xy)=2$

$\Rightarrow$ Option (a) is incorrect

For option (b)

Let $G=\left(P\left(\mathbb{N}\right),\Delta\right)$

G is an infinite group in which every element is of finite order.

For option (c)

Let $G=Q_8$

All subgroups of G are normal in G but G is non abelian.

For option (d) :

We know that if G is abelian group then all subgroup of G are normal

Correct option is (d).

6. Let $GL_n(\mathbb{R})$ denote the group of all $n \times n$ matrices with real entries (with respect to matrix multiplication) which are invertible. Pick out the normal subgroups from the following: **[NBHM-2010]**

(a) The subgroup of all real orthogonal matrices

(b) The subgroup of all invertible diagonal matrices

(c) The subgroup of all matrices with determinant equal to unity

Soln. For option (a)

Take $n=2$

Let $A=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

Clearly $A \in GL_2\left(\mathbb{R}\right)$ is an orthogonal matrix.

Let $B=\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$

Let $BAB^{-1}=\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

$=\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -2 \end{bmatrix}=\begin{bmatrix} 2 & 5 \\ -1 & -2 \end{bmatrix}$

Clearly BAB^{-1} is not an orthogonal matrix

$\Rightarrow$ The subgroup of all real orthogonal matrices does not form a normal subgroup of $GL_n\left(\mathbb{R}\right)$

For option (b):

Take $n = 2$

Let $A=\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$

Clearly A is an invertible diagonal matrix.

Let $B=\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \in GL_2\left(\mathbb{R}\right)$

Consider $BAB^{-1}=\begin{bmatrix}1 & -2\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$

$$=\begin{bmatrix}1 & -2\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 2\\ 0 & 2\end{bmatrix}=\begin{bmatrix}1 & -2\\ 0 & 2\end{bmatrix}$$

$\Rightarrow$ BAB^{-1} is not a diagonal matrix

$\Rightarrow$ The subgroup of all invertible diagonal matrices does not form a normal subgroup.

For option (c)

Let $A\in GL_n(\mathbb{R})$ be such that det (A) = 1

Let $B\in GL_n(\mathbb{R})$

Consider det $\left(BAB^{-1}\right)=\det(B)\det(A)\det\left(B^{-1}\right)$

$$=\det(B)\det(A)\frac{1}{\det(B)}=\det(A)=1$$

$\Rightarrow \det\left(BAB^{-1}\right)=1$

Thus the subgroup of all matrices with determinant equal to unity form a normal subgroup of $GL_n(\mathbb{R})$

Hence correct option is (c)

7. Let G be the group of invertible upper triangular matrices in $\mathbb{M}_2(\mathbb{R})$. If we write $A\in G$ as $A=\begin{pmatrix}a_{11} & a_{12}\\ 0 & a_{22}\end{pmatrix}$, which of the following define a normal subgroup of G? **[NBHM-2014]**

(a) $H=\{A\in G\mid a_{11}=1\}$

(b) $H=\{A\in G\mid a_{11}=a_{22}\}$

(c) $H=\{A\in G\mid a_{11}=a_{22}=1\}$

Soln. Given $G=\left\{\begin{pmatrix}a_{11} & a_{12}\\ 0 & a_{22}\end{pmatrix}\in M_2(\mathbb{R})\middle| a_{11}a_{22}\neq 0\right\}$

For option (a)

Given $H=\{A\in G\mid a_{11}=1\}$

Let $B\in G$

Let $A\in H\Rightarrow A=\begin{pmatrix}1 & a'_{12}\\ 0 & a'_{22}\end{pmatrix}; a'_{22}\neq 0$

Let $B\in G$

$\Rightarrow$ $B=\begin{pmatrix}a_{11} & a_{12}\\ 0 & a_{22}\end{pmatrix}; a_{11}a_{22}\neq 0$

Consider $BAB^{-1}=\begin{pmatrix}a_{11} & a_{12}\\ 0 & a_{22}\end{pmatrix}\begin{pmatrix}1 & a'_{12}\\ 0 & a'_{22}\end{pmatrix}\frac{1}{a_{11}a_{22}}\begin{pmatrix}a_{22} & -a_{12}\\ 0 & a_{11}\end{pmatrix}$

$$=\frac{1}{a_{11}a_{22}}\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} a_{22} & -a_{12}+a_{11}a'_{12} \\ 0 & a_{11}a'_{22} \end{pmatrix}$$

$$=\frac{1}{a_{11}a_{22}}\begin{pmatrix} a_{11}a_{22} & -a_{12}a_{11}+a_{11}^2a'_{12}+a_{12}a_{11}a'_{22} \\ 0 & a_{11}a_{22}a'_{22} \end{pmatrix}\in H$$

$\Rightarrow$ H is normal in G

For option (b)

Given $H=\{A\in G \mid a_{11}=a_{22}\}$

Let $A\in H \Rightarrow A=\begin{pmatrix} a'_{11} & a'_{12} \\ 0 & a'_{11} \end{pmatrix}; a'_{11}\neq 0$

Let $B\in G$

$\Rightarrow B=\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}; a_{11}a_{22}\neq 0$

Consider $BAB^{-1}=\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} a'_{11} & a'_{12} \\ 0 & a'_{11} \end{pmatrix}\frac{1}{a_{11}a_{22}}\begin{pmatrix} a_{22} & -a_{12} \\ 0 & a_{11} \end{pmatrix}$

$$=\frac{1}{a_{11}a_{22}}\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} a'_{11}a_{22} & -a'_{11}a_{12}+a'_{12}a_{11} \\ 0 & a_{11}a'_{11} \end{pmatrix}$$

$$=\frac{1}{a_{11}a_{22}}\begin{pmatrix} a_{11}a'_{11}a_{22} & -a_{11}a'_{11}a_{12}+a'_{12}a_{11}^2+a_{12}a_{11}a'_{11} \\ 0 & a_{11}a'_{11}a_{22} \end{pmatrix}$$

$$=\begin{pmatrix} a'_{11} & \dfrac{a'_{12}a_{11}}{a_{22}} \\ 0 & a'_{11} \end{pmatrix}\in H$$

$\Rightarrow H$ is normal in G

Similarly we can prove for option (c)

Hence correct option is (a), (b) and (c)

8. For real numbers a and b, define the mapping $\tau_{a,b}:\mathbb{R}\to\mathbb{R}$ by $\tau_{a,b}(x)=ax+b$. Let

$G=\{\tau_{a,b}:a,b\in\mathbb{R}, a\neq 0\}$

Under composition of mappings, this becomes a group. Which of the following subgroups of G are normal ?

(a) $H=\{\tau_{a,b} \mid a\neq 0, a\in\mathbb{Q}, b\in\mathbb{R}\}$ **[NBHM-2015]**

(b) $H=\{\tau_{1,b} \mid b\in\mathbb{R}\}$

(c) $H=\{\tau_{1,b} \mid b\in\mathbb{Q}\}$

Soln. Given $G=\{\tau_{a,b}:a,b\in\mathbb{R}, a\neq 0\}$

For option (a):

Given $H=\{\tau_{a,b} \mid a\neq 0, a\in\mathbb{Q}, b\in\mathbb{R}\}$

Let $x\in G\Rightarrow x=\tau_{a,b}$ for some $a,b\in\mathbb{R}, a\neq 0$

Let $h\in H\Rightarrow h=\tau_{a',b'}$ for some $a'\in\mathbb{Q}, b'\in\mathbb{R}, a'\neq 0$

Consider $xhx^{-1}=\tau_{(a,b)}\tau_{(a',b')}\tau_{(a,b)}^{-1}$

$$\tau_{(a,b)}\tau_{(a',b')}\tau^{-1}_{(a,b)}(y)=\tau_{(a,b)}\left(a'\left(\frac{y}{a}-\frac{b}{a}\right)+b'\right)$$

$$=aa'\left(\frac{y}{a}-\frac{b}{a}\right)+ab'+b$$

$$=a'(y-b)+ab'+b$$

$$=a'y+ab'-a'b+b$$

$$=\tau_{(a',\,ab'-a'b+b)}(y)\in H$$

$\Rightarrow H$ is normal in G.

For option (b)

Given $H=\{\tau_{1,b}\,|\,b\in\mathbb{R}\}$

Let $x\in G$ and $h\in H$

$\Rightarrow x=\tau_{a,b}$ for some $a,b\in\mathbb{R}$, $a\neq 0$

and $h=\tau_{1,b'}$ for some $b'\in\mathbb{R}$

Consider $\tau_{a,b}\tau_{1,b'}\tau_{\left(\frac{1}{a},\frac{-b}{a}\right)}(y)=\tau_{a,b}\tau_{1,b'}\left(\frac{1}{a}y-\frac{b}{a}\right)$

$$=\tau_{a,b}\left(\frac{1}{a}y-\frac{b}{a}+b'\right)$$

$$=a\left(\frac{1}{a}y-\frac{b}{a}+b'\right)+b$$

$$=y-b+ab'+b$$

$$=\tau_{1,ab'}(y)$$

$\Rightarrow \tau_{1,ab'}\in H$

$\Rightarrow H$ is normal subgroup of G.

For option (c):

Given $H=\{\tau_{1,b}\,|\,b\in\mathbb{Q}\}$

Let $x\in G$ and $h\in H$

$\Rightarrow x=\ \tau_{a,b}$ for some $a,b\in\mathbb{R}, a\neq 0$

and $h=\tau_{1,b'}$ for some $b'\in\mathbb{Q}$

Now $\tau_{a,b}\tau_{1,b'}\tau_{\frac{1}{a},\frac{-b}{a}}=\tau_{1,ab'}$

If $a\in\mathbb{R}-\mathbb{Q}$ then $ab'\notin\mathbb{Q}$

$\Rightarrow\ \tau_{1,ab'}\notin H$

$\Rightarrow H$ is not normal in G.

Hence correct option is (a) and (b)

9. Let $n\in\mathbb{N}, n\geq 2$. Which of the following subgroups are normal in $GL_n(\mathbb{C})$? **[NBHM-2017]**

(a) $H=\{A\in GL_n(\mathbb{C})\,|\,A \text{ is upper triangular}\}$

(b) $H=\{A\in GL_n(\mathbb{C})\,|\,A \text{ is diagonal}\}$

(c) $H=\{A\in GL_n(\mathbb{C})\,|\,\det(A)=1\}$

Soln. Given $G = GL_n(\mathbb{C})$

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

Consider $BAB^{-1} = \begin{pmatrix} 1 & -1 \\ +1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

$= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

$= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -2 & 2 \end{pmatrix}$

$= \frac{1}{2}\begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}$

Clearly BAB^{-1} is not an upper triangular matrix

$\Rightarrow H = \{A \in GL_n(\mathbb{C}) \mid A$ is upper triangular matrix$\}$ and $H = \{ A \in GL_n(\mathbb{C}) \mid A$ is diagonal$\}$ are not normal in G.

$H = \{A \in GL_n(\mathbb{C}) \mid \det(A) = 1\}$ is normal in G. $\left(\because \det(BAB^{-1}) = \det A\right)$

Hence correct option is (c)

10. Let G be an abelian group with the identity e. Which one of the following statements are true.

(a) $H = \{x \in G \mid \text{order of } x \text{ is odd}\}$ is a subgroup of G **[H.C.U. 2018]**

(b) $H = \{x \in G \mid \text{order of } x \text{ is even}\} \cup \{e\}$ is a subgroup of G

(c) Every subgroup of G is normal

(d) G is cyclic

Soln. For option (a)

Given $H = \{ x \in G \mid$ order of x is odd$\}$

To prove that H is a subgroup of G, it is sufficient to prove that H is closed

Let $a, b \in H$

$\Rightarrow o(a) =$ an odd integer and $o(b) =$ an odd integer

We know that $o(ab)$ divides lcm of $o(a)$ and $o(b)$ in an abelian group.

$\Rightarrow o(ab)$ is an odd integer

$\Rightarrow ab \in H$

$\Rightarrow H$ is a subgroup of G.

For option (b)

Take $G = \mathbb{Z}_{20}$

H = The set of all even ordered elements in $\mathbb{Z}_{20} \cup \{e\} = \{0, 1, 2, 5, ...\}$

H is not a subgroup of G. ($\because$ 1+ 5 = 6 does not belong to H)

Hence correct option is (a) and (c).

11. Any normal subgroup of order 2 is contained in the center of the group. **[TIFR-2013]**

Soln. Let G be a group and H be any subgroup of G of order 2. i.e. $H = \{e, x\}$

We have to prove $x \in Z(G)$ i.e. $xy = yx \ \forall y \in G$

Let $y \in G$ be any arbitrary element.

Since H is normal in G.

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

$\Rightarrow$ Either $yxy^{-1} = e$ or $yxy^{-1} = x$

If $yxy^{-1} = e \Rightarrow x = e$

$\Rightarrow \; yxy^{-1} \neq e$

$\Rightarrow \; y\,x\,y^{-1} = x$

$\Rightarrow \; yx = xy \;\forall\; y \in G$

$\Rightarrow x \in Z(G)$

$\Rightarrow H \subseteq Z(G)$

12. In each of the following, state whether the given set is a normal subgroup or, is a subgroup which is not normal or, is not a subgroup of $GL_n(\mathbb{C})$.

(a) The set of matrices with determinant equal to unity

(b) The set of invertible upper triangular matrices

(c) The set of invertible matrices whose trace is zero **[NBHM-2012]**

Soln. For option (a).

We know that the set of all matrices with determinant equal to unity form a normal subgroup.

For option (b):

The set of all invertible upper triangular matrices form a subgroup of $GL_n(\mathbb{C})$ but not a normal subgroup.

For option (c)

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$

Clearly A and B are invertible matrices whose trace is zero

Now $AB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\text{Trace}(AB) = 2 \neq 0$

$\Rightarrow$ The set of invertible matrices whose trace is zero does not form a subgroup of G.

13. Let A and B be normal subgroups of a group G. Suppose $A \cap B = \{e\}$, where e is the unit element of the group G, then

(a) for any $a \in A$ and $b \in B$, $ab = ba$.

(b) for only some $a \in A$ and $b \in B$, $ab = ab$.

(c) $ab \neq ba$ for any $a \in A$ and $b \in B$.

(d) $ab \neq ba$ for some $a \in A$ and $b \in B$.

Soln. Since $\forall a \in A, b \in B$

$(aba^{-1})b^{-1} \in B \,\&\, a(bab^{-1}) \in A$

as $A \bigcap B = \{e\} \Rightarrow aba^{-1}b^{-1} = e$

$\Rightarrow ab = ba \forall a \in A, b \in B$

option (a) is correct

14. Which of the following is true ?

(a) $\exists$ two subgroups H,K, which are not normal but HK is a subgroup

(b) $\nexists$ two subgroups H,K, which are not normal but HK is a subgroup

(c) If $|H|$ = 14 and |K| = 33 then $|H \cap K|$ is greater than 1

(d) A_5 has subgroup of order 15

Soln. Let $G = S_4, H = \{I, (12)\}$

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

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

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

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

Thus HK = KH $\Rightarrow$ HK is subgroup

but H and K are not normal subgroup of G

$\therefore$ option (a) is correct & (b) is false

Since $|H \cap K|$ must divide $|H| = 14$ and $|k| = 33$

$\Rightarrow |H \cap K| = 1$

$\therefore$ option (c) is false

If A_5 has subgroup of order 15. Then A_5 must have an element of order 15 as group of order 15, is cycle but A_5 does not have an element of order 15.

$\therefore$ option (d) is false

Correct option is (a)

15. Let G be a group and H, K be subgroups of G such that $G = H \oplus K$. Let N be a normal subgroup of G such that $N \cap H = \{e\}$ and $N \cap K = \{e\}$. Then N is

(a) abelian (b) Non abelian (c) Cyclic (d) None of these

Soln. Since $G = H \times K$, H and K are normal subgroup of G.

Now $\forall n \in N$, $h \in H$, $k \in K$, $nh = nh$ and $nk = kn \left\{ \begin{array}{l} \text{if H, k be normal subgroup of G \& H} \cap \text{K} = \{e\} \\ \text{then hk} = kh \ \forall h \in H \text{ and k} \in \text{K} \end{array} \right\}$

Let $a, b \in N$, then $\exists h \in H, k \in K$ such that $b = hk$.

Now $ab = a(hk) = (ah)k = (ha)k = h(ak)$

$= h(ka) = (hk)a = ba$

$\Rightarrow ab = ba$

$\Rightarrow$ N is abelian

$\therefore$ **option (a) is correct**

16. Let G be a group and $H = \left\{ g^2 \mid g \in G \right\}$. Then

(a) H must be normal subgroup

(b) H is sub group but need not to be normal subgroup

(c) H is not sub group of G.

(d) H may not be subgroup and if it is a subgroup then it must be normal.

Soln. Suppose $G = A_4$ contains all twelve even permutation of S_4 which are {I, (12)(34), (13)(24),(14)(23)} and the 8 3-cycles elements. Since $I^2 = I$, $((ab)\,(cd))^2$ = I and square of any 3-cycle is a 3-cycle, we notice H will contains I and 8-3 element cycles so that $o(H) = 9$ and $9 \nmid 12$. So H can not be subgroup of G. Option (a), (b) are false

Suppose now H is subgroup then if $h \in H, g \in G$ be any elements, then

$g^{-1} \in G \Rightarrow g^{-2} \in H$ also $gh \in G$

$\Rightarrow (gh)^2 \in H$

$\Rightarrow g^{-2}(gh)(gh) \in H$

$\Rightarrow g^{-1}hg \in H$

$\therefore$ H is normal in G.

$\therefore$ **Correct option is (d)**

Chapter 7

QUOTIENT GROUP

Quotient Group: Let H be a normal subgroup of G. If $a \in G$, then right coset Ha is same as left coset aH.

Let G/H be be the collection of all cosets of H in G i.e $G/H = \{Ha : a \in G\}$.

If $a, b \in G$, then we have $(Ha)(Hb) = H(aH)b(\because aH = Ha)$

$$= HHab = Hab$$

then the set G/H of all cosets of H in G is a group with respect to multiplication of cosets and is called quotient group of G by H.

The identity element of a quotient group G/H is H

Theorem :- Every quotient group of an abelian group is abelian

Theorem :- If H is a normal subgroup of G and $a \in G$ is of order n. If $o(Ha) = m$, then m divides n.

Theorem :- Let H_1 and H_2 be two normal subgroups of G then $G/H_1 = G/H_2$ if and only if $H_1 = H_2$

Solved Exampls

1. The quotient group $Q_8/\{1,-1\}$ is isomorphic to

(a) $(Q_8, \cdot)$ (b) $(\{1,-1\}, \cdot)$ (c) $(V_4, +)$ (d) $(\mathbb{Z}_4, +)$ **[D.U. 2014]**

Soln. Given $G = Q_8$

We know that $Z(G) = \{1, -1\}$

Also if $G/Z(G)$ is cyclic then G is abelian.

Now $o(Q_8/\{1,-1\}) = 4$

$\Rightarrow$ Either $Q_8/\{1,-1\} \approx \mathbb{Z}_4$ or $\dfrac{Q_8}{\{1,\ -1\}} \approx (V_4, +)$

But Q_8 is non abelian and $\mathbb{Z}_4$ is cyclic

$\Rightarrow Q_8/\{-1,1\} \approx (V_4, +)$

Correct option is (c)

2. Consider the following statements P and Q:

P : If H is a normal subgroup of order 4 of the symmetric group S_4, then S_4/H is abelian.

Q : If $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group, then $Q/\{-1, 1\}$ is abelian.

Which of the above statements hold TRUE ?

(a) Both P and Q (b) Only P (c) Only Q (d) Neither P nor Q

Soln. Given H is a normal subgroup of order 4 of the symmetric group $S_{4.}$

$$\Rightarrow o\left(\frac{S_4}{H}\right)=6$$

If S_4/H is abelian $\Rightarrow S_4/H$ is cyclic

$\Rightarrow S_4/H$ has an element of order 6.

$\Rightarrow S_4$ has an element of order multiple of 6 but this is not true since maximum order of an element in S_4 is 4.

$\Rightarrow S_4/H$ is not an abelian group

$\Rightarrow$ P is false

Q : Given $Q=\{\pm 1,\pm i,\pm j,\pm k\}$

$$o\left(\frac{Q}{\{-1,1\}}\right)=4$$

We know that every group of order 4 is abelian.

$\Rightarrow Q/\{-1,1\}$ is abelian

Correct option is (c)

2. Let $\omega=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$, $M=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$, $N=\begin{pmatrix}\omega & 0\\ 0 & \omega^2\end{pmatrix}$ and $G=<M,N>$ be the group generated by the matrices M and N under matrix multiplication. Then,

(a) $\frac{G}{Z(G)}\cong C_6$ (b) $\frac{G}{Z(G)}\cong S_3$ (c) $\frac{G}{Z(G)}\cong C_2$ (d) $\frac{G}{Z(G)}\cong C_4$

Soln. Given $M=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}, N=\begin{pmatrix}\omega & 0\\ 0 & \omega^2\end{pmatrix}$

$$MN=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}\omega & 0\\ 0 & \omega^2\end{pmatrix}=\begin{pmatrix}0 & i\omega^2\\ i\omega & 0\end{pmatrix}$$

$$NM=\begin{pmatrix}\omega & 0\\ 0 & \omega^2\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}=\begin{pmatrix}0 & i\omega\\ i\omega^2 & 0\end{pmatrix}$$

$\Rightarrow$ $MN\neq NM$

$\Rightarrow G$ is non abelian

we know that $G/Z(G)$ is cyclic iff G is abelian.

$\Rightarrow G/Z(G)$ can not be isomorphic to C_6, C_2, C_4

$\Rightarrow G/Z(G)\cong S_3$

Correct option is (b)

3. If $Z(G)$ denotes the centre of a group G, then the order of the quotient group $G/Z(G)$ cannot be

(a) 4 (b) 6 (c) 15 (d) 25

Soln. We know that $G/Z(G)$ is cyclic iff $G/Z(G)$ is a trivial group

If $o(G/Z(G))=15\Rightarrow(G/Z(G))$ is cyclic but $G/Z(G)$ is not a trivial group.

$\Rightarrow$ Order of $G/Z(G)$ can not be 15

Hence correct option is (c)

4. An example of an infinite group in which every element has finite order is **[H.C.U. 2010]**

(a) non-singular 2 × 2 matrices with integer entries

(b) $(\mathbb{Q}/\mathbb{Z},+)$

(c) the invertible elements in $\mathbb{Z}$ under multiplication

(d) the Quarternion group

Soln. In $\frac{\mathbb{Q}}{\mathbb{Z}}$, every element has finite order but group itself is infinite

Hence correct option is (b)

5. Consider the quotient group $G=\frac{\mathbb{Q}}{\mathbb{Z}}$ under addition. Which of the following statements about G are true?

(a) G is a finite group

(b) In G every element has a finite order

(c) G has no non-trivial proper subgroups

(d) G is NOT a cyclic group **[H.C.U-2013]**

Soln. We know that $\frac{\mathbb{Q}}{\mathbb{Z}}$, is an infinite non cyclic abelian group in which every element has finite order and for every $n\in\mathbb{N}$, there exist a unique cyclic subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$ of order n.

Here correct option is (b), (d)

6. Suppose G is a finite group and H is a subrgoup of G. If $[G : H] = 2$, then which of the following statements are true ? **[H.C.U-2018]**

(a) If $x\in H$ and $y\notin H$, then $xy\in H$

(b) If $x\notin H$ and $y\notin H$, then $xy^{-1}\in H$

(c) If $x\notin H$ and $y\notin H$, $xy\in H$

(d) both (b) and (c) are true

Soln. For option (a):

Given $x\in H$ and $y\notin H$

If $xy\in H$

$\Rightarrow xyH=H$

$\Rightarrow x^{-1}xyH=x^{-1}H$

$\Rightarrow yH=H \quad (\because x\in H\Rightarrow x^{-1}\in H)$

$\Rightarrow y\in H$

This is a contradiction.

$\Rightarrow xy\notin H$

For option (b)

Given $x\notin H$ and $y\notin H$ and H is subgroup of index 2.

$\Rightarrow xH\neq H$ and $yH\neq H$

$\Rightarrow xH=yH \qquad (\because [G:H]=2)$

Also $x^{-1}H=y^{-1}H$

$\Rightarrow H=xy^{-1}H$

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

Similarly we can prove for option (c)

Hence correct option is (b), (c) and (d)

7. Let G be a finite group and H be a subgroup of G. Let $o(G)$ and $o(H)$ denote the orders of G and H respectively. Identify which of the following statements are necessarily true. **[NBHM-2006]**

(a) If $\dfrac{o(G)}{o(H)}$ is a prime number then H is normal in G

(b) If $o(G) = 2o(H)$ then H is normal in G

(c) If there exist normal subgroup A and B of G such that $H = \{ab \mid a \in A, b \in B\}$ then H is normal in G

Soln. For option (a)

Let $G = S_3 = \{I, (12), (13), (23), (123), (132)\}$

Let $H = \{I, (12)\}$

Now $\dfrac{o(G)}{o(H)} = 3$, a prime number but H is not normal is G.

For option (b)

Given $o(G) = 2\,o(H)$

$\Rightarrow \dfrac{o(G)}{o(H)} = 2$

$\Rightarrow$ The index of H in G is 2.

$\Rightarrow$ H is normal in G.

For option (c)

Given A and B are normal subgroups of G.

Given $H = \{ab \mid a \in A, b \in B\}$

To prove H is normal in G.

Let $x \in G$ and $h \in H$

Now $h \in H \Rightarrow h = a_1 b_1$ for some $a_1 \in A$ and $b_1 \in B$

Consider $xhx^{-1} = xa_1b_1x^{-1} = xa_1x^{-1}xb_1x^{-1}$

Since A and B is normal in G.

$\Rightarrow xa_1x^{-1} \in A$ and $xb_1x^{-1} \in B$

$\Rightarrow xa_1x^{-1}xb_1x^{-1} \in H$

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

$\Rightarrow H$ is normal in G.

Hence correct option is (a), (c)

8. How many elements of order 2 are there in the group $(\mathbb{Z}/4\mathbb{Z})^3$? **[NBHM-2007]**

Soln. Given $G = (\mathbb{Z}/4\mathbb{Z})^3 \approx \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$

2	1	1	→	1
1	2	1	→	1
1	1	2	→	1
2	2	1	→	1
1	2	2	→	1
2	1	2	→	1
2	2	2	→	1

Thus there are seven elements of order 2.

9. Let H, N be subgroups of a finite group G, with N a normal subgroup of G. If the orders of G/N and H are relatively prime, then H is necessarily contained in N. **[TIFR-2019]**

Soln. Suppose H is not contained in N.

$\Rightarrow \exists\, h \in H$ such that $h \notin N$

$\Rightarrow Nh \neq N$ i.e., $o(Nh) \neq 1$

Since $Nh \in G/N$

$\Rightarrow o(Nh) \,|\, o(G/N)$

Also $o(Nh) \,|\, o(h)$

$\Rightarrow o(Nh) \,|\, o(H)$

Thus $o(Nh) \,|\, \gcd\left(o(G/N), o(H)\right)$

$\Rightarrow o(Nh) \,|\, 1$

$\Rightarrow o(Nh) = 1$

Which is a contradiction

Hence our supposition is wrong

Thus $H \subseteq N$

Thus given statement is true

10. Let H be a subgroup G such that $x^2 \in H \;\forall x \in G$, then

(a) H is normal subgroup of G and G/H is commutative.

(b) H is normal subgroup of G and G/H is not commutative.

(c) If H is proper subgroup of G such that $\forall x, y \in G/H,\; xy \in H \Rightarrow$ H is normal subgroup of G.

(d) If H is proper subgroup of G such that $\forall x, y \in G/H, xy \in H \not\Rightarrow$ H is normal subgroup of G.

Soln. Let $h \in H \Rightarrow x \in G$ such that $h = x^2$

$ghy^{-1} = yx^2g^{-1} = \left(gxg^{-1}\right)^2 = y^2 \in H$

$\Rightarrow$ H is normal in G

Let $xH, yH \in G/H$ If G/H is commutative then $xHyH = yHxH$ or $(yx)^{-1}(xy) \in H$ consider $(yx)^{-1}(xy)$.

Now $(yx)^{-1}(xy) = \left(x^{-1}y^{-1}(xy)\right) = \left(x^{-1}y^{-1}\right)^2\left(yxy^{-1}\right)^2 y^2$

Since $a^2 \in H \;\forall\, aG \Rightarrow \left(x^{-1}y^{-1}\right)^2\left(yxy^{-1}\right)^2 y^2 \in H$ and so $(yx)^{-1}(xy) \in H$. Thus G/H is commutative option (a) is correct and option (b) is false

Now, Let $x \in G/H$. Then $x^{-1} \in G/H$ let $y \in H$

$\Rightarrow \quad xyx^{-1} \in H$

$\therefore$ H is a normal subgroup of G.

$\therefore$ option (c) is correct and (d) is false

Correct option are (a) and (c)

11. Let H and K be normal subgroups of a group G. Suppose $H < K$ and G/H is abelian. Then

(a) G/K is also abelian

(b) G/K need not to be abelian

(c) G/H need not to be a subgroup of G/K

(d) None of these

Soln. From the third isomorphism theorem $\frac{G}{K} \cong \frac{G/H}{G/K}$

Since H, K are normal subgroup of G and $H< K$.

and from assumption G/H is abelian gruop. It follows G/H |G/K is an abelian group.

$\therefore$ The group G/K is an abelian group and $\frac{G}{H} < \frac{G}{K}$ iff $H < K$

$\therefore$ option (b), (c) are false

Option (a) is correct

12. Let G be a group and H, K be normal subgroup of G then

(a) If $\frac{G}{H} \cong \frac{G}{K}$ and G is cyclic then H = K

(b) If $\frac{G}{H} \cong \frac{G}{K}$ and if G is not cyclic, then H = K

(c) If $\frac{G}{H} \cong \frac{G}{K}$ and G is cyclic then H need not be equal to K.

(d) None of these

Soln. Let $G = \langle a \rangle$ and suppose $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$, then n is the smallest +ve integer such that $a^n \in H$.

Thus $H, Ha, ..., H_a^{n-1}$ are distinct right cosets of H in G.

So, $i_G(H) = n$

Similarly $i_G(K) = m$

Now, $\frac{G}{H} \cong \frac{G}{H} \Rightarrow i_G(H) = i_G(K) \Rightarrow n = m \Rightarrow H = K = \langle a^n \rangle$

$\therefore$ option (a) is true and (c) is false

Let $G \equiv Q_8$ and $H = \{\pm 1, \pm i\}, k = \{\pm 1, \pm j\}$

then H, K are normal subgroups of G.

and $\frac{G}{H} = \{H, H_j\}, \frac{G}{K} = \{K, Ki\}$

the mapping $H \to K, H_j \to K_i$ will be on isomorphism, where a $H \neq K$

$\therefore$ option (b) is false

Correct option is (a)

13. Let H and K are normal subgoups of a finite group G and $\frac{G}{H} \cong K$, then

(a) $\frac{G}{K} \cong H$

(b) $\frac{G}{H}$ need not to be isomorphic to H

(c) HK need not to be normal subgroup of *G*.

(d) If H an odd order subgroup of G. of index 2. Then H need not contains every element of G of odd order.

Soln. Let $G = Q_8$ and $H = \{\pm 1, \pm i\}$

$K = \{\pm 1\}$

obviously $H \Delta G, K \Delta G$ and G/H is cyclic of order 2 so it is isomorphic to K

but $\frac{G}{K} \cong K_4$, $\frac{G}{K} \ncong H$

So, option (b) is correct and (a) is false

If *H*,*K* are normal subgroup $\Rightarrow$ *HK* is also normal subgroup of *G*.

$\therefore$ option (c) is false

Since $\left|\frac{G}{H}\right| = 2$ $\Rightarrow$ forevery a in G $(aH)^2$ = H

(every group of odd order must contains all elements of odd order)

If *a* is an element of a order 2n+1, then

$$H = a^{2n+1}H = \left((aH)^2\right)^n aH = aH \Rightarrow a \in H$$

$\therefore$ every element of odd order $\in H \Rightarrow$ option (d) is false

Correct option is (b)

Chapter 8

Homomorphism, Isomorphism, Automorphism & Inner Automorphism &External Direct Product

1. **Isomorphic Mapping. Definition:** Suppose G and G' are two groups, the composition in each being denoted multiplicatively. A mapping *f* of *G* into G' is said to be an isomorphic mapping of *G* into G' if

(i) *f* is one-to-one i.e., distinct elements in *G* have distinct *f*-images in G',

(ii) $f(ab) = f(a)f(b) \forall a, b \in G$ i.e., the image of the product is the product of the images.

It should be noted that when we say that *f* is a mapping of *G* into G', we usually include in it the possibility that the mapping *f* may be onto G'.

If *f* is an isomorphic mapping of a group *G* into a group G', then *f* is also called an isomorphism of *G* into G'. If *f* is an isomorphism of *G* onto G', the group G' is called an isomorphic image of the group *G*.

2. **Isomorphic groups. Definition:** Suppose *G* and G' are two groups. Further suppose that the compositions in both *G* and G' have been denoted multiplicatively. Then we say that the group *G* is isomorphic to the group G' if there exists a one-to-one mapping *f* of *G* onto G' such that

$f(ab) = f(a)f(b) \forall a, b \in G$ i.e., the mapping *f* preserves the compositions in *G* and G'.

If the group *G* is isomorphic to the group G', symbolically we write $G \cong G'$.

Note 1: If *G* is isomorphic to G', there may exist more than one isomorphisms of *G* onto G'.

Note 2: If the group *G* is finite, then *G* can be isomorphic to G' only if G' is also finite and the number of elements of *G* is equal to the number of elements in G'. Otherwise there will exist no mapping *f* from *G* to G' which is one-one as well as onto.

Note 3: If the group *G* is isomorphic to the group G', then we say that the groups *G* and G' are abstractly identical. From the point of view of abstract algebra we shall regard them as one group and not as two different groups.

3. **Some more examples:**

Ex.1. If $\mathbb{R}$ is the additive group of real numbers and $\mathbb{R}^+$ the multiplicative group of positive real numbers, prove that the mapping $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x \; \forall x \in \mathbb{R}$ is an isomorphism of $\mathbb{R}$ onto $\mathbb{R}^+$.

Soln. If *x* is any real number, positive, zero or negative, then e^x is always a positive real number. Also e^x is unique. Therefore if $f(x) = e^x$ then $f : \mathbb{R} \to \mathbb{R}^+$.

***f* is one-to-one.**

Let $x_1, x_2 \in \mathbb{R}$. Then $f(x_1) = f(x_2) \quad \Rightarrow e^{x_1} = e^{x_2}$

$\Rightarrow \log e^{x_1} = \log e^{x_2} \Rightarrow x_1 \log e = x_2 \log e \Rightarrow x_1 = x_2$

Thus, two elements in $\mathbb{R}$ have the same *f*-image in $\mathbb{R}^+$ only if they are equal. Consequently distinct elements in $\mathbb{R}$ have distinct *f*-images in $\mathbb{R}^+$. Therefore *f* is one-to-one.

***f* is onto:** Suppose *y* is any element of $\mathbb{R}^+$ i.e. *y* is any positive real number. Then log *y* is a real number i.e., $\log y \in \mathbb{R}$.

Now $f(\log y) = e^{\log y} = y$. Therefore each element of $\mathbb{R}^+$ is the f-image of some element of $\mathbb{R}$. Thus f is onto.

f preserves compositions in $\mathbb{R}$ and $\mathbb{R}^+$. Suppose x_1 and x_2 are any two elements of $\mathbb{R}$. Then

$f(x_1 + x_2) = e^{x_1 + x_2}$

$= e^{x_1} e^{x_2}$

$= f(x_1) f(x_2)$ $[\because f(x_1) = e^{x_1}$ and $f(x_2) = e^{x_2}]$

Thus f preserves compositions in $\mathbb{R}$ and $\mathbb{R}^+$. Here the composition in $\mathbb{R}$ is addition and the composition in $\mathbb{R}^+$ is multiplication. Therefore f is an isomorphism of $\mathbb{R}$ onto $\mathbb{R}^+$. Hence $\mathbb{R} \cong \mathbb{R}^+$.

Ex. 2. Let $\mathbb{R}^+$ be the multiplicative group of all positive real numbers and $\mathbb{R}$ be the additive group of all real numbers. Show that the mapping $g : \mathbb{R}^+ \to \mathbb{R}$ defined by $g(x) = \log x \,\forall x \in \mathbb{R}^+$ is an isomorphism.

Soln. Let $x_1, x_2 \in \mathbb{R}^+$.

Let $g(x_1) = g(x_2)$

$\Rightarrow \log x_1 = \log x_2$

$\Rightarrow e^{\log x_1} = e^{\log x_2} \Rightarrow x_1 = x_2$

Therefore, g is one-to-one.

Suppose y is any element of $\mathbb{R}$ i.e. y is any real number. Then e^y is definitely a positive real number i.e. $e^y \in \mathbb{R}^+$.

Now $g(e^y) = \log e^y = y$.

$\Rightarrow$ there exists $e^y \in \mathbb{R}^+$ such that $g(e^y) = y$. Therefore each element of $\mathbb{R}$ is the g-image of some element of $\mathbb{R}^+$. Thus g is onto.

g preserves compositions in $\mathbb{R}^+$ and $\mathbb{R}$. Suppose x_1 and x_2 are any two elements of $\mathbb{R}^+$. Then

$g(x_1 x_2) = \log(x_1 x_2)$ [by def. of g]

$= \log x_1 + \log x_2$

$= g(x_1) + g(x_2)$ [by def. of g]

Thus g preserves compositions in $\mathbb{R}^+$ and $\mathbb{R}$. Here the composition in $\mathbb{R}^+$ is multiplication and the composition in $\mathbb{R}$ is addition. Therefore g is an isomorphism of $\mathbb{R}^+$ onto $\mathbb{R}$. Hence $\mathbb{R}^+ \cong \mathbb{R}$.

Ex.3. Show that the additive group of integers $G = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ is isomorphic to the additive group $G' = \{..., -3m, -2m, -1m, 0, 1m, 2m, 3m, ...\}$ where m is any fixed integer not equal to zero.

Soln. If $x \in G$, then obviously $mx \in G'$. Let $f : G \to G'$ be defined by $f(x) = mx \,\forall x \in G$.

Let $x_1, x_2 \in G$.

Let $f(x_1) = f(x_2)$

$\Rightarrow mx_1 = mx_2$ [by def. of f]

$\Rightarrow x_1 = x_2$ $[\because m \neq 0]$

Therefore f is one-to-one

Suppose y is any element of G'. Then obviously $y/m \in G$. Also $f(y/m) = m(y/m) = y$.

Thus, if $y \in G'$ then there exists $y/m \in G$ such that $f(y/m) = y$. Therefore each element of G' is the f-image of some element of G. Hence f is onto.

Again, if x_1 and x_2 are any two elements of G, then

$f(x_1+x_2) = m(x_1+x_2)$ [by def. of f]

$= mx_1 + mx_2$ [by distributive law for integers]

$= f(x_1) + f(x_2)$ [by definition of f]

Thus, f preserves compositions in G and G'. Therefore, f is an isomorphic mapping of G onto G'. Hence, G is isomorphic to G'.

Ex.4. Show that the set $\mathbb{C}$ of all complex numbers under addition is a group which is isomorphic to itself under the identity mapping as well as under the mapping which takes every complex number into its conjugate complex.

Soln. The identity mapping f defined by $f : \mathbb{C} \to \mathbb{C}$ such that $f(z) = z \,\forall\, z \in \mathbb{C}$ is obviously one-one onto.

Also, $f(z_1+z_2) = z_1 + z_2 = f(z_1) + f(z_2) \forall\, z_1, z_2 \in \mathbb{C}$.

$\therefore$ the identity mapping f is an isomorphism of $\mathbb{C}$ onto $\mathbb{C}$.

If $z = x + iy$ is any complex number, then $\overline{z} = x - iy$ is called the conjugate complex of z.

Let $g : \mathbb{C} \to \mathbb{C}$ be such that $g(z) = \overline{z} \,\forall z \in \mathbb{C}$

Let $z_1, z_2 \in \mathbb{C}$. Then $g(z_1) = g(z_2) \Rightarrow \overline{z}_1 = \overline{z}_2 \Rightarrow \overline{(\overline{z}_1)} = \overline{(\overline{z}_2)} \Rightarrow z_1 = z_2$

Therefore, g is one-to-one.

If $x + iy$ is any element of $\mathbb{C}$, then $x - iy$ is also an element of $\mathbb{C}$. Also $g[(x-iy] = x + iy$. Therefore g is onto.

Further, if $z_1, z_2 \in \mathbb{C}$, then $g(z_1+z_2) = \overline{(z_1+z_2)} = \overline{z}_1 + \overline{z}_2 = g(z_1) + g(z_2)$

Hence g is also an isomorphism of $\mathbb{C}$ onto $\mathbb{C}$.

4. Some important properties of isomorphic mappings:

Let f be an isomorphic mapping of a group G into a group G'. Then we have the following important properties.

(i) The f-image of the identity e of G is the identity of G' i.e., $f(e)$ is the identity of G'.

Proof: Let e be the identity of G and e' be the identity of G'. Let a be any element of G. Then $f(a) \in G'$.

Now, $e'f(a) = f(a)$ [$\because$ e' is the identity of G]

$= f(ea)$ [$\because$ e is the identity of G]

$= f(e)f(a)$ [$\because$ f is an isomorphic mapping]

Now in the group G', we have

$e'f(a) = f(e)f(a) \Rightarrow e' = f(e)$ [by right cancellation law in G']

$\therefore$ $f(e)$ is the identity of G'.

(ii) The f-image of the inverse of an element a of G is the inverse of the f-image of a i.e., $f(a^{-1}) = [f(a)]^{-1}$

Proof : Suppose e is the identity of G and e' is the identity of G'. Then $f(e) = e'$. Now let a be any element of G. Then $a^{-1} \in G$ and $aa^{-1} = e$. We have