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 $ab=ba$, $g.c.d.(o(a), o(b))=1$ 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 HK 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*) $Z(G) = \bigcap_{\forall\, a \in G} N(a)$

(*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 $GL(n, F)$

(*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 $2n$.

(*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 $d \mid n$ and $d \neq 2$, D_{2n} has exactly $\phi(d)$ element of order d.

(*vi*) For every $d \mid n$, $\exists$ 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 $b \neq c$