Euler's ϕ function.

$$\phi : N \longrightarrow N$$

$$\phi(n) = |\{x \in N \mid 1 \le x \le n,\ \gcd(x,n) = 1\}|$$

$$\phi(p^n) = p^n - p^{n-1}$$

$$\phi(mn) = \phi(m)\,\phi(n) \quad \text{if } \gcd(m,n) = 1$$

Ques: Euler ϕ function $(\phi(n))$ is one-one ?

Sol: No,

because $\phi(1) = 1$

$\phi(2) = 1$

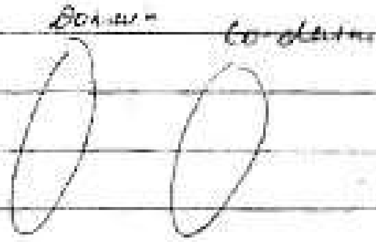
$\phi(4) = 2$

$\phi(3) = 2$

$\phi(10) = 4$

$\phi(8) = 4$

$\phi(12) = 4$



Co-domain has image more than one element so it is not one-one.

because $\phi(10) = 4 = \phi(8)$

But $10 \neq 8$ in N.

$\phi(n) =$ even if $n > 2$

$n \in N$

$\phi(n) = 3$

$3 \in N$ (Co-domain)

$n \in N$

$\phi(n) = 3$

$\phi(n)$ is not onto.

Ans: $\phi(50) = 20$,

$\phi(1000) = 400$

1×5
$2 \times 2 \times 5$
$2 \times 5^2 \cdot 2^2 \times 5$
$2 \times 5^2 - 5^{2-1}$, $2^2 - 2^1$
$4 - 2$
$2 \times 25 - 5$ 2×5
2×20

$n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$

$\tau(n) = (p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdots p_k^{\lambda_k})$

$= (\lambda_1+1)(\lambda_2+1) \cdots (\lambda_k+1)$

How many element relatively prime to 0.

Ans

$\gcd(10, 0) = 10$

because $10 = 1, 2, 5, 10$

$0 = 1, 2, \cdots 10 \cdots$

Common divisor $= 1, 2, 5, 10$

$\gcd = 10$.

$\gcd(-10, 0) = 10$

Q: How many ~~element~~ integers are relatively prime to 0.

Sol: $\gcd(0, 0) = 1$, $0 \in \mathbb{Z}$

then,

0 is relatively prime to zero.

eg. $\gcd(1, 0) = 1$

$\gcd(-1, 0) = 1$

Q: How many integers are relatively prime to 1.

Ans: Infinite.

Partition of the Set :-

A set P is called Partition of the set X if

(i) $\phi \notin P$

(ii) $\bigcup_{A \in P} A = X$

(iii) if $A \in P$, $B \in P$, and $A \neq B$ then $A \cap B = \phi$

e.g. $X = \{a, b, c\}$

Possibility in (1) $(3) \rightarrow \{a, b, c\}$

" " 2. $(2+1) \rightarrow$ (i) $\{a, b\}, \{c\}$ (ii) $\{a, c\}, \{b\}$
(iii) $\{a\}, \{b, c\}$

" " 3. $1+1+1 \rightarrow \{a\}, \{b\}, \{c\}$.

~~No of~~

Note:- Set containing $n+1$ elements then number of the partition the set - $\boxed{P(n+1) = \sum_{r=0}^{n} {}^{n}C_{r} P(r)}$

$P(0) = 1$

$P(1) = 1$

Q. Set containing two elements then the partition

$$P(2) = P(1+1) = \sum_{r=0}^{1} {}^{1}C_{r} P(r)$$

$P(0) = 1$

$P(1) = 1.$

Sol:- $P(1+1) = {}^1C_0 P(0) + {}^1C_1 P(1)$

$= 1 + 1$

$= 2.$

$\left\{ {}^nC_r = \dfrac{n!}{r!\,(n-r)!} \right.$

Ques: If set containing three elements then $P(3) = ?$

Sol: $P(3) = P(2+1) = \sum_{r=0}^{2} {}^2C_r \, P(r)$

$= {}^2C_0 P(0) + {}^2C_1 P(1) + {}^2C_2 P(2)$

$= 1 + 2 + 1 \cdot 2$

$= 5$

Ques: If set containing four element then $P(4)$?

Sol: $P(4) = P(3+1) = \sum_{r=0}^{3} {}^3C_r \, P(r)$

$= {}^3C_0 P(0) + {}^3C_1 P(1) + {}^3C_2 P(2) + {}^3C_3 P(3)$

$= 1 + 3 + 6 + 5$

$= 15$

\# $P(1)$ 1

$P(2)$ 1 → 2

$P(3)$ 2 3 → 5

$P(4)$ 5 7 10 → 15

$P(5)$ 15 20 27 37 → 52

Que: $U(8) = \{1, 3, 5, 7\}$ Show that $U(8)$ is group with respect to multiplication modulo 8.

Sol:- closure:

$\forall\ a \in U(8), \forall\ b \in U(8)$

$ab \in U(8)$

By table

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

(ii) Associative.

$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall\ a, b, c \in U(8)$

(iii) Identity.

$\forall\ a \in U(8)\ \exists\ 1 \in U(8)$ such that

$a\cdot 1 = 1\cdot a = a \quad \forall\ a \in U(8)$

(iv) Inverse: $\forall\ a \in$

$ax \equiv 1 \pmod 8$

$1x \equiv 1 \pmod 8$

$3x \equiv 1 \pmod 8$

$1^{-1} = 1$

$3^{-1} = 3$

$5^{-1} = 5$

$7^{-1} = 7.$

then $(U(8), \cdot)$ is Group

$O(U(8)) = 4$

Now find order of each elements of $U(8)$

$O(1) = 1$

$O(3) = 2$

$O(5) = 2$

$O(7) = 2$

$(3\cdot 3 = 3^2 = 9 = 1$

$\Rightarrow O(3) = 2$

Que: find possible order of elements in

U(8), and how many.

Sol: Possible order of elements in U(8) = 1 & 2

# of element of order 1 in U(8) = 1

# of element of order 2 in U(8) = 3

Ques: find possible order of element in U(15) and How many. Done *

Ques: Show that U(n) is group w.r.t. multiplication modulo n.

Sol: $a \in U(n)$ {a is member of U(n)} {a & n are relative prime}

for inverse

$ax \equiv 1 \pmod{n}$ has unique solution.

(1) Closure

$\forall a \in U(n), \forall b \in U(n)$

$\Rightarrow a \cdot b \in U(n)$

(2) Associative law

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

$\forall a, b, c \in U(n)$

(3) $\forall a \in U(n) \ \exists \ 1 \in U(n)$

such that $a \cdot 1 = 1 \cdot a = a$

(4) for each $a \in U(n)$ they $a^{-1} \pmod{n} \in U(n)$

s.t. $aa^{-1} = a^{-1}a = 1$.

a is relative prime two number in integer is relative prime infinite no. in integer

$(2,7) = 1$

$7 = 2 \times 3 + 1$ → gcd

$2 = 1 \times 2 + 0$

$1 = 7 \times 1 - 2 \times 3$

$1 = 7 \times 1 + 2 \times (-3)$ — (1)

$2x \equiv 1 \pmod{7}$

$2x = 1 + 7k$

$\Rightarrow 2x - 7k = 1$

$\Rightarrow 2x + 7(-k) = 1$

$2x + 7k_1 = 1$ — (2)

from (1) & (2)

$x = -3$

$k_1 = 1$.

then $U(n)$ is group.

*Ques:- find possible order of elements in $U(15)$ and also find number of elements of possible order in $U(15)$.

Sol:-

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

$O(U(15)) = 8$

$1 \in U(15)$ such that $O(1) = 1$

$2 \in U(15)$ such that $O(2) = 4$

$4 \in U(15)$ " " $O(4) = 2$ $4 \times 4 = 1$

$7 \in U(15)$ " " $O(7) = 4$

$8 \in U(15)$ " " $O(8) = 4$

$11 \in U(15)$ " " $O(11) = 2$

$13 \in U(15)$ " " $O(13) = 4$

$14 \in U(15)$ " " $O(14) = 2$

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

# of elements of order 1 in $U(15) = 1$
" " " " 2 " " $= 3$
" " " " 4 " " $= 4$

$\phi(n)$

Ques: find possible order of element in $U(31)$ and how many.

Sol: Possible order of elements in $U(31) = 1, 2, 3, 5, 6, 10, 15, 30$

No. of elements of order 1 in $U(31) = 1$
" " 2 " " $= 1$
" " 3 " $U(31) = 2$
5 " " $= 4$
6 " " $= 2$
10 " " $= 4$
15 " " $= 8$
30 " " $= 8$

Ques: find possible order of element in $U(50)$ and how many.

$Z_{20} \oplus Z_{10}$

Ques: Show that D_4 is group under composition?

Sol:

$$D_4 = \{x^i y^j \mid x^2 = e,\ y^4 = e,\ xy = y^{-1}x,\ i = 0,1,\ j = 0,1,2,3\}$$

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

1. Closure property

$\forall\, a \in D_4,\ \forall\, b \in D_4$

$\Rightarrow a \cdot b \in D_4$ (from composition table of D_4)

(2) Associative.

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \qquad \forall\, a,b,c \in D_4$$

(3) Identity: $\forall\, a \in D_4$, $R_0 \in D_4$ such that

$$a \circ R_0 = R_0 \circ a = a.$$

(4) Inverse: Inverse of each element of D_4

$$R_0^{-1} = R_0$$

$$R_{90}^{-1} = R_{270}$$

$$R_{180}^{-1} = R_{180}$$

$$R_{270}^{-1} = R_{90}$$

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

$$V^{-1} = V$$

$$D^{-1} = D$$

$$D'^{-1} = D'$$

Then D_4 is Group w.r.t. Composition.

Now $O(D_4) = 2\cdot 4 = 8.$

Next find possible order of element in D_4

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

$O(R_{90}) = 4$

$O(R_{180}) = 2$

$O(R_{270}) = 4$

$O(H) = 2$

$O(V) = 2$

$O(D) = 2$

$O(D') = 2$

identity has order 1

possible order of elements in D_4 are 1, 2 and 4

# of elements of order 1 in $D_4 = 1$
2 in $D_4 = 5$
4 in $D_4 = 2$

Ques. Show that D_n is group with respect to composition.

Ques. Find possible order of elements in D_3

$D_3 = \{R_0, R_{120}, R_{240}, f_{AA}, f_{BB}, f_{CC}\}$

$O(D_3) = 2 \cdot 3 = 6$

$O(R_0) = 1$
$O(R_{120}) = 3$
$O(R_{240}) = 3$
$O(f_{AA}) = 2$
$O(f_{BB}) = 2$
$O(f_{CC}) = 2$

Reflection order always 2.

Possible order elements in D_3 are 1, 2 and 3

Next.
No. of elements of order 1 in $D_3 = 1$
" " " 2 " " = 3
" " " " 3 " " = 2

Q: Possible order of elements in D_1 1 and 2

$D_1 = \{R_0, f_0\}$
$O(D_1) = 2 \cdot 1 = 2$
$O(R_0) = 1$
$O(f_0) = 2$

then possible order of elements in $D_1 = 1 \& 2$.

# of elements of order 1 in D_1 = 1

" " " " " 2 in D_1 = 1

Q: find possible order of elements in D_{10}.

Sol:

[Since rotation = reflection]

No. of rotation = No. of reflection

Q: find possible order of elements in Z_{10}.

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

$O(0) = 1$

$O(1) = 10$ $\quad 1 \in 10$

$O(2) = 5$ $\quad 1+1+\cdots+1 = 10$. Z_{10} mean under addition

$O(3) = 10$

$O(4) = 5$ $\quad O(2) = 5$

$O(5) = 2$

$O(6) = 5$

$O(7) = 10$

$O(8) = 5$

$O(9) = 10$

Possible order of elements in Z_{10} are 1, 2, 5 & 10

# of elements of order 1 in Z_{10} = 1

2 " " = 1

5 " " = 4

10 " " = 4

Scanned with CamScanner

Note: If d/n then # no. of element of order d in $Z_n = \phi(d)$

16/08/2014.

Note:- 1. # of elements of order 2 in D_n = $(n+1)$ if n is even; $= n$ if n is odd

2. If $2 \nmid d/n$, then the # of elements of order d in $D_n = \phi(d)$

Ques: Possible order of elements in D_{33}.

Sol:- Possible order of elements in D_{33} are 1, 2, 3, 11 and 33.

$2 \nmid 1/33$ then the # of elements of order 1 in $D_{33} = \phi(1) = 1$

" " " " 2 in $D_{33} = 33$

$2 \nmid 3/33$ then the # of elements of order 3 in $D_{33} = \phi(3) = 2$

$2 \nmid 11/33$ " " " " " " order 11 in $D_{33} = \phi(11) = 10$

$2 \nmid 33/33$ " " " " " " " 33 in $D_{33} = \phi(33) = 20$

$O(D_{33}) = 66$

Ques:- Possible order of elements in z.

Sol: $z = \{0, \pm 1, \pm 2, \pm 3 \ldots\}$

$1 \cdot 0 = 0$ then $o(0) = 1$

$1 \in z$ such that $o(1) = \infty$

if $0 \neq a \in z$ then $o(a) = \infty$

then possible order of elements in $z = 1$ and ∞

{Only one element finite in z}

{ a^{e} ko kitne bar bhi add karo identity nahi milegi }

$\therefore o(a) = \infty$

Ques:- How many element of order finite in z

Sol: Exactly one element of order finite in z say 0 means order of identity in z is 1

Ques:- Possible order of elements in Q

" R

" C

Similar as z

Ques:- Possible order of elements in Q^*.

Sol:- Q^* is group under multiplication the $a \in Q^*$ and $o(a) = n$, $a^n = 1$ and n is least positive integer.

Scanned with CamScanner

$1 \in Q^*$ such that $1^1 = 1$ then $O(1) = 1$
$-1 \in Q^*$ such that $(-1)^2 = 1$ then $O(-1) = 2$

$2 \in Q^*$ such that $O(2) = \infty$

Ques: How many element of order finite in Q^*.

Ans: Two elements of order finite Any 1 and -1.

Ques: Possible order of element in $\mathbb{R}^*$
Same as Q^*

Ques: Possible order of element in C^*

Sol: $(1)^{1/n} \in C^*$ s.t. $O((1)^{1/n}) = 1$

$(1)^1$
$1^1 = 1$
$(i)^2 = i$
$(i)^4 = 1$
$(-i)^4$

Note: Infinite number of element in C^* of order finite.

Ques: Show that $G l_n(F)$ is group under multiplication

Proof: $G l_n(F) = \{A = [a_{ij}]_{n \times n} \mid |A| \neq 0, a_{ij} \in F\}$

1. $A \in G l_n(F) \Rightarrow |A| \neq 0$
$B \in G l_n(F) \Rightarrow |B| \neq 0$

$|A \cdot B| = |A| \cdot |B|$
$\neq 0$

$$\left\{ \begin{array}{l} 0 \neq 2 \in Z_6 \\ 0 \neq 3 \in Z_6 \\ 2 \cdot 3 = 6 = 0 \end{array} \right.$$

then $A \cdot B \in Gl_n(F)$

(ii) $A(B \cdot C) = (A \cdot B) \cdot C \quad \forall\ A, B, C \in Gl_n(F)$

(iii) $\forall\ A \in Gl_n(F)$, $\exists\ I_n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{n \times n} \in Gl_n(F)$

such that
$$A \cdot I_n = I_n A = A.$$

(iv) $A \in Gl_n(F) \Rightarrow |A| \neq 0$ then $A^{-1} = \frac{adj A}{|A|}$

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

then $A^{-1} \in Gl_n(F)$

$Gl_n(F)$ is Group w.r.t multiplication.

Ques: Show that $Sl_n(F)$ is group under multiplication.

Proof:-

for (iv) $A \in Sl_n(F) \Rightarrow |A| = 1$

So

$$|A^{-1}| = \frac{1}{|A|} = \frac{1}{1} = 1$$

Ques: Show that quaternion (Q_4) is group with respect to multiplication.

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

Scanned with CamScanner

Sol: (1) & (2) property hold
(closure & associative)

① from table closure property hold.

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	+1
-k	-k	k	-j	+j	+i	-i	+1	-1

② Associative law

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

$\forall a, b, c \in Q_4$

③ $\forall a \in Q_4 \ \exists 1 \in Q_4$

such that $a\cdot 1 = 1\cdot a = a$

④ Inverse of each element of Q_4

$1^{-1} = 1$

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

$(i)^{-1} = -i$

$(-i)^{-1} = i$

$(j)^{-1} = -j$

$(-j)^{-1} = j$

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

$(-k)^{-1} = k$. Hence Q_4 is a group w.r.t. multiplication.

Ques: Possible order of elements in Q_4.

Sol: $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$

$1 \in Q_4$ such that $O(1) = 1$

$-1 \in Q_4$ " " $O(-1) = 2$

$i \in Q_4$ " " $O(i) = 4$

$-i \in Q_4$ such that $O(-i) = 4$

$j \in Q_4$ " " $O(j) = 4$ $\{ \because j^2 = -1$
$j^4 = j^2 \cdot j^2$
$= (-1)(-1)$
$= 1$

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

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

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

Possible order of element in $Q_4 = 1, 2, 4$.

# of elements of order 1 in $Q_4 = 1$
# of elements of order 2 in $Q_4 = 1$
# of elements " " 4 in $Q_4 = 6$

Klein's 4- Group:

It is denoted by K_4

$K_4 = \{e, a, b, ab \mid a^2 = e, b^2 = e, ab = ba\}$

① **Closure property**

satisfy from table.

$\forall x \in K_4$
$\forall y \in K_4$
such that $xy \in K_4$

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

② **Associative.**

$x(y \cdot z) = (x \cdot y) \cdot z \quad \forall \; x, y, z \in K_4$

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

RGB

Red → Blue.

(iii) $\forall\ x \in K_4\ \exists\ e \in K_4$ such that $x \cdot e = ex = x$

(iv) Inverse of each element of K_4

$$e^{-1} = e$$
$$a^{-1} = a$$
$$b^{-1} = b$$
$$ab^{-1} = ab^{-1}$$

$(ab)^e = e$
$(ab)(ab) = e$
$ab = ab^{-1}$

Then K_4 is group of order 4 with identity e.

Possible order of elements in K_4 1 and 2.

Ques: Is $R+G+B$ Group ?

Sol:
$f_1 : R+G+B \to R+G+B$
$f_2 : R+G+B \to R-G+B$
$f_3 : R+G+B \to R+G-B$
$f_4 : R+G+B \to R-G-B$

$f_2 f_1 = f_2(R+G+B)$
$= R-G+B$
$f_3 f_2 = f_3(R-G+B)$
$R-G-B = f_4$

~~$\{f_1, f_2, f_3, f_4\}$~~

Here f_1 is identity $\{\because f_2 f_1 = f_2\}$
& f_2, f_3, f_4 have self inverse.

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Abelian Group:- A Group G is said to be abelian group if $a \underset{\text{operation}}{*} b = b * a \quad \forall a, b \in G$

Example:

$(Z,+)$ is abelian Groups —

Solution:

Yes, $a+b = b+a \quad \forall a, b \in Z$.

Ques:- Is $(Q,+)$ $(R,+)$ $(C,+)$ $(Q^*,\cdot)$ $(R^*,\cdot)$ $(C^*,\cdot)$ all abelian Group.

Sol:- Yes all these are abelian group.

Ques:- $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$ is abelian ?

Sol:- No, $i \in Q_4$, $j \in Q_4$

$ij = k \neq ji$ then Q_4 is not abelian.

Ques:- $D_4 = \{x^i y^j \mid x^2 = e, y^n = e, xy = y^{-1}x;\ i = 0,1, j = 0,1,2 \ldots n-1\}$

Is this abelian group.

* D_n abelian is dependent on

$D_n = \{x^i y^j \mid x^2 \ldots\}$ is abelian.

Sol:- If $n \leq 2$

Put $n = 1$

$D_1 = \{x^i y^j \mid x^2 = e, y = e, xy = y^{-1}x, i = 0,1, j = 0\}$

$xe = e^{-1}x$

$\Rightarrow xe = ex \qquad y = e$

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

$\Rightarrow D_1$ is abelian

$\{ R_{90} H = \theta,\ H R_{90} = H',\ R_{90} H \neq H R_{90} \}$

Scanned with CamScanner

Put $n = 2$ then

$D_2 = \{x^i y^j \mid x^2 = e, y^2 = e, xy = y^{-1}x, i = 0,1, j = 0,1\}$

But:

$$y^2 = e \Rightarrow y \cdot y = e \Rightarrow y = y^{-1} \quad -(1)$$

from relation $xy = y^{-1}x$

$\Rightarrow xy = yx$

Now If $n \geq 3$ then D_n is always non abelian.

Que: $Gl_n(F)$ is abelian?

Sol: Need not be abelian

If $n = 1$ then { for $n=1$ abelian }

$Gl_n(F) = \{ A = [a_{ij}]_{1\times1} \mid |A| \neq 0, a_{ij} \in F\}$

Suppose $F = \mathbb{R}$ then

$Gl_n \mathbb{R} = \{ A = [a] \mid |A| \neq 0, a \in \mathbb{R}\}$

$= \mathbb{R}^*$

$\mathbb{R}^*$ is abelian group w.r.t multiplication then $Gl_1(\mathbb{R})$ is abelian group of order ∞.

(ii) If $n \geq 2$ then

$Gl_n(F)$ is non abelian group

Que: $Sl_n(F)$ is abelian

Sol: 1. If $n = 1$ then $Sl_n(F)$ is abelian { Scalar matrix Commute with all matrix }

(iv) If $n \geq 2$ then $SL_n(F)$ is non-abelian.

Que: $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid 0 \neq a \in \mathbb{R} \right\}$ is Group w.r.t. multiplication.

Sol. $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid 0 \neq a \in \mathbb{R} \right\}$

$$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G \quad B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$$

$$A \cdot B = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$$

$\left\{ \begin{array}{l} a \in \mathbb{R} \\ b \in \mathbb{R} \\ a \cdot b \in \mathbb{R} \end{array} \right.$

(ii) Associative law

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \quad \forall A, B, C \in G$$

(iii) Let $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ is the identity of G then

$$A \cdot B = A$$

$$\Rightarrow \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$$\Rightarrow 2ab = a$$

$$\Rightarrow b = \frac{1}{2}$$

then $B = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$ is the identity of G

(iv) Suppose $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ inverse of $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$.

then

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$\begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$\Rightarrow 2ab = \frac{1}{2}$$

$$b = \frac{1}{4a}, \quad 0 \neq a \in \mathbb{R}$$

then $B = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$.

Hence $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} / 0 \neq a \in R \right\}$ is Group w.r.t. multiplication.

{Need not Group}.

{If det is zero then G is need not be Group }we satisfy closure, ass. inverse identity exit we not see det zero hai ya nahi}

Ques: $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} / 0 \neq a \in \mathbb{R} \right\}$ is group, w.r.t multiplication

{Define on it}

Sol: (1) Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in G$,

$$B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \in G$$

$$A \cdot B = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} \in G, \quad 0 \neq a \in \mathbb{R}, \; 0 \neq b \in \mathbb{R}$$

$\Rightarrow 0 \neq a \cdot b \in \mathbb{R}$

(ii) Associative:

$$A\cdot(B\cdot C) = (A\cdot B)\cdot C \quad \forall\ A, B, C \in G$$

(iii) let $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ is identity of G then

$$A\cdot B = A$$

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

$$\Rightarrow \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow ab = a$$

$$\Rightarrow b = 1$$

then $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

(iv) $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ is the inverse of $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$ab = 1$$

$$b = 1/a$$

then $B = \begin{bmatrix} 1/a & 0 \\ 0 & 0 \end{bmatrix}$

then G is a Group under multiplication.

Ques. $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid 0 \neq a \in Z \right\}$ is this Group.

Sol: No, it is not group because in inverse we have $a = 1/a$

$1/a \notin Z$

Ques: $G = Z$

$a \circ b = a + b + 1$; $a, b \in Z$ then $(G, \circ)$ is group ?

Sol: ① $\forall\, a \in Z$, $\forall\, b \in Z$

$a \circ b = a + b + 1 \in Z$

then $a \circ b \in Z$

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

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

$= a + b + c + 1 + 1$

$= a + b + c + 2$

R.H.S

$(a \circ b) \circ c = (a + b + 1) \circ c$

$= a + b + 1 + c + 1$

$= a + b + c + 1 + 1$

$= a + b + c + 1$

$\left\{ \begin{array}{l} (Z, +) \text{ is Commutative} \\ \therefore 1 + c = c + 1 \end{array} \right.$

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

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

$\forall\ a, b, c \in Z.$

(iii) identity:

b is the identity of G

then $a \circ b = a$

$\Rightarrow a + b + 1 = a$

$\Rightarrow b = -1$

(iv) Inverse

Suppose b is the inverse of a then

$a \circ b = -1$

$a + b + 1 = -1$

$b = -2 - a$

then $(G, \circ)$ is Group.

Que: $G = Q^+ \rightarrow$ Set of all positive rational number

$a \circ b = \frac{ab}{3}$

$(G \circ)$ is Group? (Group) Do yourself

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

$\left(\frac{ab}{3}\right) \circ c = a \circ \frac{bc}{3}$

$\frac{abc}{3 \cdot 3} = \frac{abc}{3 \cdot 3}$

Que: $G = Q^- \rightarrow$ Set of all negative rational number

$a \circ b = \frac{ab}{3}$

$(G \circ)$ is Group? {Not a group}

Sol: Not a group because

$-1 \in Q^{-1}$

$-2 \in Q^{-1}$

$(-1) \circ (-2) = \frac{(-1)(-2)}{3} = \frac{2}{3} \notin Q^{-1}$

then $(G \circ)$ is not Group.

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

Sol:- Let G be a Group and $O(a) = n \Rightarrow a^n = e$ —(1)

$(xax^{-1})^2 = (xax^{-1})(xax^{-1}) = xax^{-1}xax^{-1}$

$= xa(x^{-1}x)ax^{-1}$ (By associativity)

$= xaeax^{-1}$

$= xa^2x^{-1}$

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

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

$= xa^2x^{-1}xax^{-1}$

$= xa^2eax^{-1}$

$= xa^2ax^{-1}$

$= xa^3x^{-1}$

||ly

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

$= xex^{-1}$ from (1)

$= xx^{-1}$

$= e$

Since n is least positive integer then

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

$\Rightarrow O(a) = O(xax^{-1})$.

||ly $O(a) = O(x^{-1}ax)$ Do yourself ...?

then

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

Scanned with CamScanner

Ques: Show that $O(ab) = O(ba)$ $\forall$ $a, b \in G$

Proof:- $ab = abe$

$= abaa^{-1}$

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

$O(ab) = O(a(ba)a^{-1})$

$\{ \because O(x(ba)x^{-1}) = O(ba) \}$

$= O(ba)$

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

then $O(ab) = O(ba)$.

Ques: Show that $(ab)^{-1} = b^{-1}a^{-1}$ $a, b \in G$

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

$\Rightarrow (ab)(b^{-1}a^{-1}) = e$ (By associativity) $\left\{ \begin{array}{l} e = bb^{-1} \\ \because a^{-1} = abb^{-1}b^{-1} \end{array} \right\}$

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

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

Ques: Show that $O(a) = O(a^{-1})$?

Sol:- Let $O(a) = n$

$\Rightarrow a^n = e$

Taking inverse on both side

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

$\Rightarrow a^{-n} = e$

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

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

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

$Z_{10} = \{0, 1, 2, 3 \dots 9\}$

$O(1) = 10$

$O(9) = 10$

$O(2) = 5$

$O(8) = 5$

$O(3) = 10 = O(7)$

Q: Every elements of G has self inverse then G is abelian but converse need not be true?

Proof:- Let G be a group and every elements of G has self inverse

Let $a \in G \Rightarrow a^{-1} = a$ (i)

$b \in G \Rightarrow b^{-1} = b$ -(ii)

$a \in G,\ b \in G \Rightarrow \underset{\text{operation}}{a \cdot b} \in G \Rightarrow (ab)^{-1} = ab$

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

$\Rightarrow ba = ab$

(from (i) & (ii))

then G is abelian.

Ques: $a^2 = e$ $\forall a \in G$ then G is ~~abtea~~ abelian but converse need not true

Sol. $a \cdot a = e \Rightarrow a = a^{-1}$

But converse need not be true

$Z_4 = \{0, 1, 2, 3\}$

$0^{-1} = 0$

$1^{-1} = 3$ $\quad\{a + n - a$

$2^{-1} = 2$

$3^{-1} = 1$

Only 0 & 2 are self inverse of Z_4 but Z_4 is abelian. Group.

Ques:

20/08/2014.

Q:- Show that

$$K_4 = \{e, a, b, ab \mid a^2 = e,\ b^2 = e,\ ab = ba\}$$

is abelian.

Sol:- $e \in K_4$ such that $e^{-1} = e$

$a \in K_4$ such that $a^{-1} = a$

$b \in K_4$ such that $b^{-1} = b$

$ab \in K_4$ such that $(ab)^{-1} = ab$

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

$(ab)^2 = e$
$\Rightarrow ab = (ab)^{-1}$

Since every element of K_4 has self inverse then K_4 is abelian.

Que: If a is commute with b then a^{-1} is also commute with b.

Sol. Let G be a group and a is commute with b.

i.e $ab = ba \qquad a, b \in G$

$\Rightarrow b = a^{-1}ba$

$\Rightarrow \boxed{ba^{-1} = a^{-1}b.}$

Que: If a is commute with b then a^{-1} is also commute with b^{-1}.

i.e. $ab = ba \Rightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$ H.W.

Scanned with CamScanner

Ans:- $(ab)^2 = a^2b^2$ iff G is abelian, $a, b \in G$

Proof. If G is abelian then

$$ab = ba \quad \text{—(1)} \quad \forall\ a, b \in G$$

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

Conversely:-

$$(ab)^2 = a^2b^2$$
$$\Rightarrow \cancel{a}b\,a\cancel{b} = \cancel{a}ab\cancel{b}$$

$$\Rightarrow ab = ba \quad \forall\ a, b \in G$$

then G is abelian.

Ans: If $(ab)^{-1} = a^{-1}b^{-1}$, iff G is abelian.

Sol: If G is abelian then

$$ab = ba$$
$$(ab)^{-1} = b^{-1}a^{-1}$$
$$= b^{-1}aa^{-1}a^{-1}$$
$$=$$

H.W.

Cyclic Group:-

A Group G is said to be cyclic group if there exist element $a \in G$ s.t. every elements of G generated by a

i.e.

$$G = \{a^n \mid n \in \mathbb{Z}\}$$

i.e.

$$G = \langle a \rangle$$

Example: $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is cyclic group?
(under addition)

Sol: $1 \in Z_6$ such that 1

$1+1 = 2$

$1+1+1 = 3$

$1+1+1+1 = 4$

$1+1+1+1+1 = 5$

$1+1+1+1+1+1 = 6 = 0$

then 1 is generator of Z_6
i.e.

$$\boxed{G = Z_6 = \langle 1 \rangle}$$

$5 \in Z_6$ such that 5

$5+5 = 4$

$5+5+5 = 3$

$5+5+5+5 = 2$

$5+5+5+5+5 = 1$

$5+5+5+5+5+5 = 0$

then 5 is generator of Z_6
i.e.

$$\boxed{G = Z_6 = \langle 5 \rangle}$$

1 & 5 are generator of Z_6
Z_6 is cyclic group.

Ques: If G is cyclic then G is abelian.

Proof: Let G is cyclic group then $\exists\, a \in G$ such that
$G = \langle a \rangle$

Suppose $x \in G$ then $x = a^n$ $n \in \mathbb{Z}$
$y \in G$ " $y = a^m$ $m \in \mathbb{Z}$

$$xy = a^n \cdot a^m \qquad n \in \mathbb{Z}$$
$$= a^{n+m} \qquad m \in \mathbb{Z}$$
$$= a^{m+n} \qquad n+m = m+n$$
$$= a^m \cdot a^n \qquad \text{because } \mathbb{Z} \text{ is}$$
$$= y \cdot x \qquad \text{abelian}$$

$\Rightarrow x \cdot y = y x \quad \forall\, x, y \in G$

then G is abelian.

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

$$K_4 = \{e, a, b, ab \,/\, a^2 = e,\ b^2 = e,\ ab = ba\}$$

$a \in K_4$

$$\left.\begin{aligned} a^1 &= a \\ a^2 &= e \\ a^3 &= a \\ a^4 &= e \end{aligned}\right\}$$

$\Rightarrow$ a generator only two elements of K_4 say a and e then a is not Generator of K_4

Illy b and ab are also not generator of K_4

$b^1 = b$ and $ab^1 = ab$
$b^2 = e$ $\quad (ab)^2 = e$

then K_4 is not cyclic but K_4 is abelian.

Scanned with CamScanner

~~Note:~~

Obs: (i) If $O(a)=n \Rightarrow a^n=e$ But Converse need not be true.

(ii) If $a^n=e \Rightarrow O(a)/n$, $a \in G$.

Proof (ii) Suppose $a^n=e$ then $O(a)/n$ and

$$O(a)=k \Rightarrow a^k=e \quad -(1)$$

By division algorithm

$$n=kq+r \quad -(3)$$

$$0<r<k$$

if $r \neq 0$ then

$$e=a^n=a^{kq+r}$$

$$=a^{kq}.a^r$$

$$=(a^k)^q.a^r$$

$$=(e)^q.a^r \quad \text{from eq}^n (1)$$

$$=a^r$$

$$e=a^r$$

$\Rightarrow a^r=e$,

But k is least positive integer then $r \neq 0$ is not possible

$\Rightarrow r=0$

from eq^n (3)

$$n=kq+r$$

$$n=kq+0$$

$$\Rightarrow k/n$$

$$\Rightarrow O(a)/n.$$

(i) If $a \in G$ then $a^{O(G)}=e$

i.e. $O(a)/O(G)$

Scanned with CamScanner

Ques:- Show that $\mathbb{Z}$ is cyclic group w.r.t. under addition.

Sol: $\mathbb{Z} = \{0, \pm 1, \pm 2 \cdots\}$

{Z is under addition then $a^n = na$}

$a = 1 \in \mathbb{Z}$ such that $G = \langle 1 \rangle$
$= \{na \mid n \in \mathbb{Z}\}$ [∵
$= \{n \cdot 1 \mid n \in \mathbb{Z}\}$

then 1 is generator of $\mathbb{Z}$
then
$G = \mathbb{Z}$ is cyclic

Now $-1 \in \mathbb{Z}$ such that
$G = \mathbb{Z} = \langle -1 \rangle$
$= \{n(-1) \mid n \in \mathbb{Z}\}$
then (-1) also generator of $\mathbb{Z}$

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

Ques: $(Q, +)$ is cyclic
$(R, +)$ is cyclic
$(C, +)$ is cyclic
$(Q^*, \cdot)$ is cyclic
$(R^*, \cdot)$ " "
$(C^* \cdot)$ " "
?

Sol:- $a \notin Q$
such that
$Q = \langle a \rangle$.
$= \{n \cdot a \mid n \in \mathbb{Z}\}$ Not cyclic.

Ques: $U(12) = \{1, 5, 7, 11\}$ is cyclic?

Sol:- $1 \in U(12)$ such that $O(1) = 1$
$5 \in U(12)$ such that $O(5) = 2$
$7 \in U(12)$ " " $O(7) = 2$
$11 \in U(12)$ " " $O(11) = 2$

$O(U(12)) = 4$ and $U(12)$ has no element of order 4 then $U(12)$ is not cyclic.

Ques: D_1 is cyclic?

Solution: $O(D_1) = 2 \cdot 1 = 2$ and D_1 has element of order of 2 then D_1 is cyclic.

Ques: D_2 is cyclic?

Sol: $O(D_2) = 2 \cdot 2 = 4$ and D_2 has no element of order 4 then D_2 is not cyclic

Ques: $D_n, n \geq 3$ is non abelian then D_n is non cyclic.

Ques: $GL_n(F)_{n>1}$ is cyclic?

Solution: $GL_n(F) = \{ A = [a_{ij}]_{n \times n} \mid a_{ij} \in F$ and $|A| \neq 0 \}$

$GL_n(F)$ is non abelian (matrix multiplication is not ~~abelian~~)

then $GL_n(F)$ is not cyclic.

Ques: If $n=1$ then $GL_1(R) = ?$

Sol: If $n=1$ then $GL_1(R) = R^*$.

and R^* is abelian but not cyclic

$\Rightarrow GL_1(R)$ is abelian but not cyclic.

Ques: 1. $SL_n(F)$, $n>1$ is cyclic?

2. If $n=1$ then $SL_n(F)$ is cyclic?

Sol: (1) $SL_n(F)$ is non-abelian if $n \geq 2$ then $SL_n(F)$ is not cyclic

(ii) If $n=1$ then $SL_1(F) = \{A = [a_{ij}] \mid |A| = 1, a_{ij} \in F\}$

$= \{[1]\}$ order of this element is 1.

$O(SL_1(F)) = 1$ and $SL_1(F)$ has element of order 1 then $SL_1(F)$ is cyclic.

Ques: $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$ is cyclic?

Sol: $i \in Q_4$ and $ij = -ji \neq ji$

$j \in Q_4$ i.e. $ij \neq ji$ then Q_4 is non abelian

$\Rightarrow Q_4$ is not cyclic.

Que: Show that Z_n is cyclic?

Sol: If $n = 1$ then $Z_1 = \{0\}$

and $O(Z_1) = 1$, $0 \in Z_1$ such that $O(0) = 1$

$\Rightarrow Z_1$ has element of order 1 then Z_1 is cyclic.

if $n \geq 2$ then $1 \in Z_n$ such that $O(1) = O(Z_n)$ then Z_n is cyclic.

Z_4

$\phi(x) =$

Note: Number of generator in $Z_n = \phi(n)$, if $\gcd(a, n) = 1$ and $a \in Z_n$ then a is generator of Z_n

Que: How many generator in Z_{20}

Sol: $Z_{20} = \{1, 2, 3, \ldots 19\}$

# of generator in $Z_{20} = \phi(20) = 8$ ~~say~~ $1, 3, 7, 9, 11, 13, 17, 19$.

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

Sol: $G = \{5, 15, 25, 35\}$

Table

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

(i) from table closure property satisfy. $a \cdot b \in G \ \forall a, b \in G$. Identity

(ii) Associative is also satisfy. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall a, b, c \in G$

(iii). 25 is identity.
$\forall a \in G \ \exists \ 25 \in G$ s.t.
$a \cdot 25 = 25 \cdot a = a$

(iv) Inverse of each element of G

$5^{-1} = 5$

$15^{-1} = 15$

$25^{-1} = 25$

$35^{-1} = 35$

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

G is abelian w.r.t. to multiplication

Every elements of G has self inverse then G is abelian

G is cyclic - No.
$O(G) = 4$ but G has no element of order 4 then G is not cyclic.

Note:- G has only one element of order 1 and 3 element of order 2.

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

Table:

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

Every element of U(8) has self inverse $\begin{pmatrix} 1^{-1} = 1 \\ 3^{-1} = 3 \\ 5^{-1} = 5 \\ 7^{-1} = 7 \end{pmatrix}$ then

U(8) is abelian group of order 4.

Now U(8) is not cyclic because U(8) has no element of order 4.

U(8) has only one element of order 1 & 3 element of & order 2 then

$$\boxed{G \approx U(8)}$$

Que:- $Z_2 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$\{0,1\} \quad \{0,1\}$

$\{Z_2$ take group under addition$\}$

Que:- find possible order of elements $Z_2 \times Z_2$

Sol:- $G = Z_2 \times Z_2$

$d_1 \quad d_2$

$\mathrm{Lcm}(d_1, d_2) = K$ and $d_1 | 2$ and $d_2 | 2$

$\mathrm{Lcm}(d_1, d_2)$ is possible if $Z_2 \times Z_2$

$Z_2 \times Z_2$

$LCM(1,1) = 1 \quad 1 \quad 1 \quad \phi(1)\,\phi(1) = 1 \cdot 1 = 1$

then number of elements of order 1 in $Z_2 \times Z_2 = 1$

Now $LCM(d_1, d_2) = 2$ also possible if

$Z_2 \times Z_2$

$d_1 | 2, \ d_2 | 2 \quad LCM(2,1) = 2 \quad 2 \quad 1 \quad \phi(2)\,\phi(1) = 1 \cdot 1 = 1$

$d_1 | 2, \ d_2 | 2 \quad LCM(1,2) = 2 \quad 1 \quad 2 \quad \phi(1)\,\phi(2) = 1 \cdot 1 = 1$

$d_1 | 2, \ d_2 | 2 \quad LCM(2,2) = 2 \quad 2 \quad 2 \quad \phi(2)\,\phi(2) = 1$

$+ \underline{3}$

Q: Possible order of element $Z_2 \times Z_4$

Sol: # of elements of order 1 in $Z_2 \times Z_4$

$1/2, 1/4 \quad LCM(1,1) = 1 \leftarrow 1 \quad 1 \quad \phi(1)\,\phi(1) = 1 \cdot 1 = 1$

then only one element of order 1 in $Z_2 \times Z_4$

# of elements of order 2 in $Z_2 \times Z_4$

$LCM(1,2) = 2 \leftarrow 1 \quad 2 \quad \phi(1)\,\phi(2) = 1 \cdot 1 = 1$

$LCM(2,1) = 2 \leftarrow 2 \quad 1 \quad \phi(2)\,\phi(1) = 1 \cdot 1 = 1$

$LCM(2,2) = 2 \leftarrow 2 \quad 2 \quad \phi(2)\,\phi(2) = 1 \cdot 1 = 1$

$= 3$

# of elements of order 4 in $Z_2 \times Z_4$

$1/2, 4/4 \quad LCM(1,4) = 4 \leftarrow 1 \quad 4 \quad \phi(1)\,\phi(4) = 2$

$2/4, 4/4 \quad LCM(2,4) = 4 \leftarrow 2 \quad 4 \quad \phi(2)\,\phi(4) = 2$

$= 4$

1/2 · 1/4 $\text{Lcm}(1,1) = 1 \leftarrow$ 1 1 $\phi(1)\,\phi(1) = 1\cdot 1 =$

$$\boxed{\begin{array}{l} K \text{ in } Z_m \times Z_n \\ \text{if} \\ \text{Lcm}(d_1, d_2) = K \text{ and } d_1 | m,\ d_2 | n \\ \qquad \sum \phi(d_1)\,\phi(d_2) \end{array}}$$

Note: No. of elements of order K in $Z_m \times Z_n$
$= \sum \phi(d_1)\,\phi(d_2)$
such that
$\text{Lcm}(d_1, d_2) = K$ and $d_1 | m$ and $d_2 | n$

Ques: How many elements of order 2 in $Z_2 \times Z_2 \times Z_2$

Sol: $G = Z_2 \times Z_2 \times Z_2$

2 1 1 $\phi(2)\,\phi(1)\,\phi(1) = 1\cdot 1\cdot 1 = 1$
1 2 1 $\phi(1)\,\phi(2)\,\phi(1) = 1\cdot 1\cdot 1 = 1$
1 1 2 $\phi(1)\,\phi(1)\,\phi(2) = 1\cdot 1\cdot 1 = 1$
2 2 1 $\phi(2)\,\phi(2)\,\phi(1) = 1\cdot 1\cdot 1 = 1$ $= 7$
2 1 2 $\phi(2)\,\phi(1)\,\phi(2) = 1\cdot 1\cdot 1 = 1$
1 2 2 $\phi(1)\,\phi(2)\,\phi(2) = 1\cdot 1\cdot 1 = 1$
2 2 2 $\phi(2)\,\phi(2)\,\phi(2) = 1\cdot 1\cdot 1 = 1$

then 7 element of order 2 in G

Ques: How many elements of order 1 in $Z_2 \times Z_2 \times Z_2$

Sol 1 1 1 $\phi(1)\,\phi(1)\,\phi(1) = 1\cdot 1\cdot 1 = 1$

Scanned with CamScanner

Ques: How many elements of order 10 in $Z_{10} \times Z_{20}$

Sol: $Z_{10} \times Z_{20}$

10	1
1	10
10	$\cancel{10}$ 2
5	2
2	5
10	2
2	10

or $Z_{10} \times Z_{20}$

10	1	$\phi(10)\ \phi(1) = 4 \cdot 1 = 4$
1	10	$\phi(1)\ \phi(10) = 1 \cdot 4 = 4$
10	2	$\phi(10)\ \phi(2) = 4 \cdot 1 = 4$
2	10	$\phi(2)\ \phi(10) = 1 \cdot 4 = 4$
10	10	$\phi(10)\ \phi(10) = 4 \cdot 4 = 16$
5	2	$\phi(5)\ \phi(2) = 4 \cdot 1 = 4$
2	5	$\phi(2)\ \phi(5) = 1 \cdot 4 = 4$
10	5	$\phi(10)\ \phi(5) = 4 \cdot 4 = 16$
5	10	$\phi(5)\ \phi(10) = 4 \cdot 4 = 16$

Ques: How many elements of order 5 in $Z_{10} \times Z_2$

Sol: $Z_{10} \times Z_2$

5	1	$\phi(5)\ \phi(1) = 4$
1	5	$\phi(1)\ \phi(5) = 4$

Scanned with CamScanner

Que: find possible order of elements in $Z_5 \times Z_4$.

Sol:- $G = Z_5 \times Z_4$, possible order of elements in G are $\{1, 2, 4, 5, 10, 20\}$

No. of elements of order 1 in $Z_5 \times Z_4$

$1 \quad 1 \qquad \phi(1)\,\phi(1) = 1$

# of element of order 2 in $Z_5 \times Z_4$

$1 \quad 2 \qquad \phi(1)\,\phi(2) = 1 \cdot 1 = 1$

# of element of order 4 in $Z_5 \times Z_4$

$1 \quad 4 \qquad \phi(1)\,\phi(4) = 1 \cdot 2 = 2$

# of element of order 5 in $Z_5 \times Z_4$

$5 \quad 1 \qquad \phi(5)\,\phi(1) = 4 \cdot 1 = 4$

" " " " 10 in $Z_5 \times Z_4$

$5 \quad 2 \qquad \phi(5)\,\phi(2) = 4 \cdot 1 = 4$

" " " 20 " $Z_5 \times Z_4$

$5 \quad 4 \qquad \phi(5)\,\phi(4) = 4 \cdot 2 = 8$

20

Que: find possible order of element in $Z_2 \times D_3$.

22/08/2014

Q: Possible order of elements in $Z_5 \times Z_{10}$

Sol:- Possible order of element in Z_5 = 1 and 5

Possible order of element in Z_{10} = 1, 2, 5 and 10

Possible order of element in $Z_5 \times Z_{10}$ = LCM(1,1) = 1

LCM(1,2) = 2   LCM(1,5) = 5 , LCM(1,10) = 10.

LCM(5,1) = 5.   LCM(5,2) = 10,   LCM(5,5) = 5

LCM(5,10) = 10

~~then~~ then # possible order of element in $Z_5 \times Z_{10}$ = 1, 2, 5 & 10

# of elements of order 1 in $Z_5 \times Z_{10}$

1 1 $\phi(1)\phi(1)$

= 1·1 = 1

# of elements of order 2 in $Z_5 \times Z_{10}$

1 2 $\phi(1)\phi(2)$ = 1·1 = 1

# of elements of order 5 in $Z_5 \times Z_{10}$

5 1 $\phi(5)\phi(1)$ = 4

1 5 $\phi(1)\phi(5)$ = 4

5 5 $\phi(5)\phi(5)$ = 16

24

# of elements of order 10 in $Z_5 \times Z_{10}$

1 10 $\phi(1)\phi(10)$ = 4

5 10 $\phi(5)\phi(10)$ = 16

5 2 $\phi(5)\phi(2)$ = 4

24

Scanned with CamScanner

$O(Z_5 \times Z_{10})$ = # of elements of order 1 + # of elements of order 2 + # of elements of order 5 + # of elements of order 10

$1 + 1 + 24 + 24 = 50$

Ques: $G = (Z_2 \times Z_2) = \{(0,0), (0,1), (1,0), (1,1)\}$ is abelian but not cyclic.

Sol.

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$(0,0)\cdot(0,0) = (0+0, 0+0) = (0,0)$

$(0,0)\cdot(0,1) = (0+0, 0+1) = (0,1)$

$(0,0)\ (1,0) = (0+1, 0+0) = (1,0)$

$(0,1)\ (0,1) = (0+0, 1+1) = (0,2) = (0,0)$

$\forall\ x \in Z_2 \times Z_2$

$\forall\ y \in Z_2 \times Z_2$

$x \cdot y = y \cdot x$

$(0,0)^{-1} = (0,0)$

$(0,1)^{-1} = (0,1)$

$(1,0)^{-1} = (1,0)$

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

Every element of $Z_2 \times Z_2$ has self inverse then $Z_2 \times Z_2$ is abelian.

Now, $O(Z_2 \times Z_2) = O(Z_2) \times O(Z_2)$
$= 2 \times 2$
$= 4$

But no. of element in $Z_2 \times Z_2$ of order 4 then $Z_2 \times Z_2$ is abelian but not cyclic.

$O(0,0) = 1$ $\quad$ $O(1\ 0) = 2$
$O(0\ 1) = 2$ $\quad$ $O(1\ 1) = 2$

Ques: Show that $Z_2 \times Z_3$ is cyclic.

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

$$O(Z_2 \times Z_3) = 6$$

$O(0\ 0) = 1$
$O(0\ 1) = 3$ $\quad$ $(01) = (01)]\ [(0,1)\ (0,1) = (0,2)$
$O(0\ 2) = 3$ $\quad$ $(0,1)\ (0,1)\ (0,1)$
$O(1\ 0) = 2$ $\quad$ $= (0,3)$
$O(1\ 1) = 6$ $\quad$ $= (0,0)$
$O(1\ 2) = 6$ $\quad$ $(1,1)$

$O(Z_2 \times Z_3) = O(Z_2) \times O(Z_3)$
$= 2 \times 3$
$= 6$

And $Z_2 \times Z_3$ has elements of order 6 then $Z_2 \times Z_3$ is cyclic group of order 6.

Scanned with CamScanner

$o(1)$ in $z_2 = 2$

$(1,2) \in z_2 \times z_3$

$o(2)$ in $z_3 = 3$

$o(1,2)$ in $z_2 \times z_3 = \text{lcm}(2,3) = 6$.

<u>Note:</u> $O(a,b)$ in $Z_m \times Z_n = \text{LCM}(O(a) \text{ in } Z_m, O(b) \text{ in } Z_n)$

e.g. $Z_2 \times Z_4$ ..

$(1,1) \in Z_2 \times Z_4$

$O(1,1)$ in $Z_2 \times Z_4 = \text{LCM}(2,4) = 4$

<u>Ques:</u> $G = Z_2 \times Z_4$ and $(1,1) \in Z_2 \times Z_4$ find $O(1,1) = ?$

<u>Sol:</u> $O(1,1)$ in $Z_2 \times Z_4$

$= \text{Lcm}(O(1) \text{ in } Z_2, O(1) \text{ in } Z_4)$

$= \text{Lcm}(2,4)$

$= 4$

<u>Ques:</u> find order $(1,2)$ in $Z_{50} \times Z_{100}$?

<u>Sol:</u> $O(1,2)$ in $Z_{50} \times Z_{100}$

$= \text{Lcm}(O(1) \text{ in } Z_{50}, O(2) \text{ in } Z_{100})$

$= \text{Lcm}(50, 50)$

$= 50$

<u>Ques:</u> Show that $Z_m \times Z_n$ is abelian.

<u>Proof:</u> $G = Z_m \times Z_n = \{(a,b) / a \in Z_m, b \in Z_n\}$ —(1)

let $x = (a_1, b_1) \in Z_m \times Z_n$, $a_1 \in Z_m$, $b_1 \in Z_n$

and $y = (a_2, b_2) \in Z_m \times Z_n$, $a_2 \in Z_m$, $b_2 \in Z_n$

$x \cdot y = (a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$= (a_2+a_1 \ , \ b_2+b_1)$

$= (a_2, b_2)\ (a_1, b_1)$

$= y \cdot x$

$\left\{ \begin{array}{l} a_1 \in Z_m \ , \ a_2 \in Z_m \\ \text{and} \quad Z_m \text{ is abelian} \\ \text{then} \quad a_1+a_2 = a_2+a_1 \\ \text{||ly} \quad b_1+b_2 = b_2+b_1 \end{array} \right.$

$xy = yx \quad \forall \ x, y \in Z_m \times Z_n$
then
$Z_m \times Z_n$ is abelian.

Ques: $G = Z_{15} \times Z_{20}$ is abelian?

Sol:- Yes.

Note:- $Z_m \times Z_n$ is cyclic group of order $m.n$ iff $\gcd(m,n) = 1$.

Proof:- If

$\gcd(m,n) = 1$ then

$\gcd(m,n) \cdot \text{lcm}(m,n) = m.n$

$1 \cdot \text{lcm}(m,n) = m.n$

$\Rightarrow \boxed{\text{lcm}(m,n) = mn}$ — (1)

$Z_m \times Z_n$

$a_1 \quad a_2$

$m \quad n \longrightarrow \text{lcm}(m,n) = m.n$ (since $\gcd(m,n)=1$)

then $Z_m \times Z_n$ has elements of order $\text{lcm}(m,n) = m.n = O(Z_m \times Z_n)$ then $Z_m \times Z_n$ is cyclic group of order $m.n$

Ques:- find possible order of elements in $Z_{25} \times Z_2 = Z_{25}$;

$Z_{50} = Z_{25 \cdot 2}$

Solution:- Possible order of elements in $Z_{25} \times Z_2$

" " " " " $Z_{25} = 1, 5, 25$

" " " " " $Z_2 = 1, 2$

Possible order of elements in $Z_{25} \times Z_2$ are
$Lcm(1,1) = 1$, $Lcm(1,2) = 2$, $Lcm(5,1) = 5$,
$Lcm(5,2) = 10$
$Lcm(25,1) = 25$, $Lcm(25,2) = 50$

then Possible order of elements in $Z_{25} \times Z_2$ are 1, 2, 5, 10, 25 & 50.

# of elements of order 1 in $Z_{25} \times Z_2$
1 1 $\phi(1)\,\phi(1) = 1 \cdot 1 = 1$

# of elements of order 2 in $Z_{25} \times Z_2$
1 2 $\phi(1)\,\phi(2) = 1 \cdot 1 = 1$

# of elements of order 5 in $Z_{25} \times Z_2$
5 1 $\phi(5)\,\phi(1) = 4 \cdot 1 = 4$

" " " " 10 " $Z_{25} \times Z_2$
5 2 $\phi(5)\,\phi(2) = 4$

" " " " 25 " $Z_{25} \times Z_2$
25 1 $\phi(25)\,\phi(1) = 2$

Scanned with CamScanner

# of elements of order 50 in $Z_{25} \times Z_2$

$25 \quad 2 \quad \phi(25)\,\phi(2)$

$= 20 \cdot 1$

$= 20.$

$G = Z_{50}$

$1/50$ then the # of elements of order 1 in Z_{50}

$= \phi(1) = 1$

$2/50$ " " " " " " " 2 in Z_{50}

$= \phi(2) = 1$

$5/50$ " " " " " " " 5 " "

$= \phi(5) = 4$

$10/50$ " " " " " " " 10 " "

$= \phi(10) = 4$

$25/50$ " " " " " " " 25 " "

$= \phi(25) = 20$

$50/50$ " " " " " " " 50 " "

$= \phi(50) = 20$

then $Z_{25} \times Z_2 \approx Z_{50}$

Note:- $\boxed{Z_m \times Z_n \approx Z_{m \cdot n} \quad \text{iff } \gcd(m,n) = 1}$

Ques: $G = Z_2 \times S_3$ find possible order of element & order of each element.

Scanned with CamScanner