IMS™
(INSTITUTE OF MATHEMATICAL SCIENCES)
IAS/IFoS MATHEMATICS by K. Venkanna

CYCLIC GROUPS

Set-IV

Cyclic group:

Suppose G is a group and there is an element $a \in G$ such that $G = \{a^n / n \in Z\}$ then G is called a cyclic group and 'a' is called generator of G and G is denoted by $\langle a \rangle$ or (a) or $\{a\}$.

i.e, $G = \langle a \rangle$ or (a) or $\{a\}$

i.e, a group consisting of elements which are only the powers of a single element belonging to it is a cyclic group.

Note:

- If G is a cyclic group generated by a, then the elements of G will be $\ldots a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots$ in multiplicative notation. and the elements of G will be $\ldots -2a, -a, 0, a, 2a, \ldots$ in additive notation.
- The elements of G are not necessarily distinct.

There exist finite and infinite cyclic groups.

Ex: ① $G = \{1, -1\}$ is $\times^{ve}$ group.

Since $(-1)^0 = 1$, $(-1)^1 = -1$.

$\therefore G = \{(-1)^0, (-1)^1\}$

$\therefore (G, \cdot)$ is a cyclic generated by -1

i.e, $G = \langle -1 \rangle$

② $G = \{\ldots\ldots -4, -2, 0, 2, 4, \ldots\ldots\}$ is an additive group.

Since $G = \{2m / m \in I\}$

$= \{\ldots\ldots -4, -2, 0, 2, 4, \ldots\ldots\}$

$\therefore G$ is a cyclic group generated by 2.

i.e, $G = \langle 2 \rangle$.

HEAD OFFICE: 25/8, OLD RAJENDER NAGAR, DELHI-60. | 011-45629987, 9999197625

(3) $G=\{1,-1,i,-i\}$

Since $G=\{(i),(i)^2,(i)^3,(i)^4\}$

$\therefore$ G is a cyclic group generated by i.

i.e, $G=\langle i\rangle$.

Similarly $G=\langle -i\rangle$.

(4) $G=\{1,\omega,\omega^2\}$ is a cyclic group. and $G=\langle\omega\rangle$, $G=\langle\omega^2\rangle$.

Note: There may be more than one generators of a cyclic group.

Ex: Suppose G is any group and $a\in G$.

Let H be the subgroup of G consisting of all integral powers of 'a'.

i.e, $H=\{a^n / n\in I\}$ then H is a cyclic subgroup of G generated by 'a'.

Ex: Show that the set of all n^{th} roots of unity w.r.t x^n is a cyclic group.

Sol^n: $1^{1/n}=(\cos 0+i\sin 0)^{1/n}$

$=(\cos 2k\pi+i\sin 2k\pi)^{1/n}$

$=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$;

$k=0,1,2,\ldots\ldots(n-1)$

$=e^{\frac{2k\pi i}{n}}$; $k=0,1,2,\ldots n-1$.

Let $G=\{e^{\frac{2k\pi i}{n}} / k=0,1,2,3,\ldots n-1\}$

which is a group under x^n.

Let $G=\{w^0=e, w^1, w^2, \ldots\ldots w^{n-1}\}$

where $w^k=e^{\frac{2k\pi i}{n}}$, $k=0,1,2,\ldots\ldots(n-1)$

Since $w^0=1=e$, $w^1=w$, $w^2=w^2$, $\ldots\ldots$ $w^{n-1}=w^{n-1}$.

$\therefore$ Every element of G is some power of w.

i.e, $G=\langle w\rangle$,

i.e $G=\langle e^{\frac{2\pi i}{n}}\rangle$.

→ Let $A=\begin{bmatrix}1&0\\0&1\end{bmatrix}$, $B=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$ $C=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$ and $D=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$

we have that $G=\{A,B,C,D\}$ with matrix multiplication as operation is a group whose composition table is given below.

•	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

Sol^n: Here $O(G)=4$

A is the identity element in G.

Now $B^1=B$, $B^2=B\cdot B=C$

$B^3=B^2\cdot B=C\cdot B=D$

$B^4=B^3\cdot B=D\cdot B=A$

$\therefore B\in G$ generates the group G and hence G is a cyclic group with B.

i.e., $G=\langle B\rangle$

→ Describle all the elements in cyclic subgroup of multiplicative group G of 2×2 matrices over $\mathbb{R}$ generated by the given 2×2 matrix.

(a) $\begin{bmatrix}0&-1\\-1&0\end{bmatrix}$ (b) $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ (c) $\begin{bmatrix}3&0\\0&2\end{bmatrix}$ (d) $\begin{bmatrix}0&-2\\-2&0\end{bmatrix}$

Sol^n: (b) Let $A=\begin{bmatrix}1&1\\0&1\end{bmatrix}$

Now $A^2=\begin{bmatrix}1&2\\0&1\end{bmatrix}$, $A^3=\begin{bmatrix}1&3\\0&1\end{bmatrix}$, ------

$A^{-1}=\begin{bmatrix}1&-1\\0&1\end{bmatrix}$, $A^{-2}=(A^2)^{-1}=\begin{bmatrix}1&-2\\0&1\end{bmatrix}$, ------

Let $H=\left\{\begin{bmatrix}1&n\\0&1\end{bmatrix} / n\in\mathbb{Z}\right\}$

$= \{A^n / n \in \mathbb{Z}\} \subseteq G$

Clearly which is subgroup of G and hence it is cyclic subgroup of G generated by A.

d) Let $A = \begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$

$A^2 = \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$, $A^3 = \begin{bmatrix} 0 & -8 \\ -8 & 0 \end{bmatrix}$, $A^4 = \begin{bmatrix} 16 & 0 \\ 0 & 16 \end{bmatrix}$, $A^5 = \begin{bmatrix} 0 & -32 \\ -32 & 0 \end{bmatrix}$

$\therefore$ All the matrices of the form

$\begin{bmatrix} 4^n & 0 \\ 0 & 4^n \end{bmatrix}$ or $\begin{bmatrix} 0 & -2^{2n+1} \\ -2^{2n+1} & 0 \end{bmatrix}$ for $n \in \mathbb{Z}$.

Let $H = \{A^n / n \in \mathbb{Z}\} \subseteq G$.

Clearly which is subgroup of G and hence it is a cyclic subgroup of G generated by A.

→ Find the order of the cyclic subgroup of the given group generated by the indicated element.

(a) The subgroup of $\mathbb{Z}_4$ generated by 3.

(b) The subgroup of U_6 generated by $\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

(c) The subgroup of U_5 generated by $\cos\frac{2\pi}{5} + i\sin\frac{4\pi}{5}$

(d) The subgroup of U_8 generated by $\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}$

(e) The subgroup of U_8 generated by $\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}$.

(f) The subgroup of the x^{ve} group of invertible 4×4 matrices generated by $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

(g) The subgroup of the x^{ve} group G of invertible 4×4 matrices generated by

(i) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ (ii) $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Soln:

(a) Let Z_4 be the set of all residue classes modulo 4 is a group w.r.t $+^n$ of residue classes.

Let $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ or $Z_4 = \{0, 1, 2, 3\}$.

Let $H = \langle 3 \rangle$

= the subgroup generated by 3

$= \{n(3) / n \in I\}$

$= \{\ldots\ldots -2(3), -1(3), 0(3), 1(3), 2(3), \ldots\ldots\}$

Now $0(3) = 0$

$1(3) = 3$

$2(3) = 3+3 = 2$

$3(3) = 3+3+3 = 1$

$4(3) = 12 = 0$ etc.

$\therefore H = \langle 3 \rangle$

$= \{0, 1, 2, 3\}$ is the cyclic subgroup of Z_4 generated by 3.

$\therefore O(H) = 4$ (or $o(H) = o$(generator) i.e, $o(H) = o(3) = 4$)

(b) $U_6 = \{z \in C / z^6 = 1\}$ i.e, $z = 1^{1/6}$

where $z = \cos\frac{2m\pi}{6} + i\sin\frac{2m\pi}{6}$;

$m = 0, 1, 2, 3, 4, 5$.

Let $U_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ $(\because \omega^6 = 1)$

U_6 is the sixth roots of unity with $e = 1$.

Let $\omega^2 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

Let $H = \langle \omega^2 \rangle$

= the subgroup generated by ω^2.

$= \{(\omega^2)^n / n \in I\}$

$= \{\ldots\ldots (\omega^2)^{-2}, (\omega^2)^{-1}, (\omega^2)^0, (\omega^2)^1, (\omega^2)^2, \ldots\ldots\}$

Now $(\omega^2)^0 = 1$

$(\omega^2)^1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

$(\omega^2)^2 = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)^2$

$= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$ (By DeMoivre's theorem)

$= \cos\left(\pi + \frac{\pi}{3}\right) + i\sin\left(\pi + \frac{\pi}{3}\right)$

$= -\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}$.

$\neq 1$

$(\omega^2)^3 = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)^3$

$= \cos 2\pi + i\sin 2\pi$

$= 1 = e$.

$(\omega^2)^4 = (\omega^2)^3(\omega^2)$

$= 1 \cdot \omega^2 = \omega^2$

$(\omega^2)^5 = (\omega^2)^4(\omega^2) = \omega^2 \cdot \omega^2 = (\omega^2)^2$

$(\omega^2)^6 = (\omega^2)^5 \cdot (\omega^2) = (\omega^2)^2 \cdot (\omega^2) = (\omega^2)^3 = 1$

$(\omega^2)^{-1} = \cos\left(-\frac{2\pi}{3}\right) + i\sin\left(-\frac{2\pi}{3}\right)$

$= \cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3}$

$= \cos\left(\pi - \frac{\pi}{3}\right) - i\sin\left(\pi - \frac{\pi}{3}\right)$

$= -\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}$

$= (\omega^2)^2$ etc.

$\therefore H = \langle \omega^2 \rangle$

$= \{1, \omega^2, (\omega^2)^2\}$ is the cyclic subgroup of U_6 generated by $\omega^2 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$.

$\therefore o(H) = 3$ (or $o(H) = o(\text{generator})$ i.e., $o(H) = o(\omega) = 3$).

Soln (f) Let $G = \{(a_{ij})_{4\times 4}\}$ is the $\times^{ve}$ group of invertible 4×4 matrices.

Let $A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

Let $H = \langle A \rangle$

= the subgroup of G generated by A.

$= \{A, A^2, A^3, \ldots\ldots\}$

Now $A^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

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

$= I$

$A^3 = A^2 \cdot A = I \cdot A = A$

$A^4 = A^3 \cdot A = A \cdot A = A^2 = I$ etc.

$\therefore H = \langle A \rangle$

$= \{I, A\} = \{A^2, A\}$ or $\{A, A^2\}$ is cyclic subgroup of G generated by A.

$\therefore O(H) = 2 = O(A)$.

→ Show that $(Z_5, +)$ where Z_5 is the set of all residue classes modulo 5, is a cyclic group w.r.t $+^n$ of residue classes.

Sol^n: Let $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ or $Z_5 = \{0, 1, 2, 3, 4\}$

Since $0 \in Z_5$

Now $1(0) = 0$

$2(0) = 0 + 0 = 0$ etc.

$\therefore 0$ is not generator of Z_5.

Since $1 \in Z_5$

Now $1(1) = 1$

$2(1) = 1 + 1 = 2$

$3(1) = 1 + 1 + 1 = 3$; $4(1) = 1 + 1 + 1 + 1 = 4$.

$5(1) = 0$; $6(1) = 1$ etc.

$\therefore \mathbb{Z}_5 = \langle 1 \rangle$

Similarly $\mathbb{Z}_5 = \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$.

$\therefore (\mathbb{Z}_5, +)$ is a cyclic group.

→ Show that $(\mathbb{Z}_m, +)$, where $\mathbb{Z}_m$ is the set of all residue classes modulo 'm' (prime) and + is the residue class $+^n$, a cyclic group.

Sol^n Let $\mathbb{Z}_m = \{0, 1, 2, \ldots\ldots m-1\}$

Now $1(1) = 1$

$2(1) = 1+1 = 2$

$3(1) = 1+1+1 = 3$

$\ldots\ldots$

$(m-1)(1) = m-1$

$m(1) = m = 0$ etc.

$\therefore$ 1 is the generator of $(\mathbb{Z}_m, +)$

i.e, $(\mathbb{Z}_m, +) = \langle 1 \rangle$.

$\therefore (\mathbb{Z}_m, +)$ is a cyclic group generated by 1.

Similarly we can prove that $2, 3, \ldots\ldots m-1$ are also generators.

Some properties of cyclic groups:

Theorem: Every cyclic group is an abelian group.

proof: Let G be the cyclic group generated by 'a'.

$\therefore G = \langle a \rangle$

$= \{a^n / n \in I\}$

Let $a^r, a^s \in G$ where $r, s \in I$

$\therefore a^r . a^s = a^{r+s} = a^{s+r}$ ($\because r+s = s+r$ in I)

$= a^s . a^r$.

$\therefore$ G is abelian

Note: The converse of the above theorem need not be true. i.e, every abelian group need not be cyclic group.

Ex: Let $G = \{A, B, C, D\}$

where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

and the matrix multiplication as the binary composition on G.

Construct composition table:

	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

Clearly G is finite abelian group (of order 4) with identity element A.

Also $B^2 = A$, $C^2 = A$ and $D^2 = A$.

i.e, each element is of order 2 (except the identity A)

Here there is no element of order 4 in G.

$\therefore$ G is not cyclic and hence every finite abelian group need not be cyclic.

→ If 'a' is a generator of a cyclic group G, then $\bar{a}^1$ is also a generator of G.

(OR)

If $G = \langle a \rangle$ then $G = \langle a^{-1} \rangle$.

Proof: Given that $G = \langle a \rangle$.

$= \{ a^n / n \in I \}$

Let $a^r \in G$; $r \in I$ then $a^r = (\bar{a}^1)^{-r}$; $-r \in I$.

$\therefore$ Each element of G is generated by $\bar{a}^1$.

$\therefore$ $\bar{a}^1$ is also generator of G. i.e, $G = \langle a^{-1} \rangle$

Theorem → Show that the number of generators of an infinite cyclic group is two.

proof: Let G be any infinite cyclic group generated by a.

$\therefore G = \langle a \rangle$

$= \{ a^n / n \in I \}$

$= \{ a^n / n = 0, \pm 1, \pm 2, \ldots \}$

Since G is infinite

$\therefore a^n = e \Leftrightarrow n = 0$ —— (1)

(**Note:** $a^m = e$ for $m \neq 0 \in Z$

$\Rightarrow G = \{ a, a^2, a^3, \ldots a^m = e \}$ which is finite)

Let $b \in G$ be any other generator of G.

$\therefore G = \langle b \rangle$

Since $b \in G = \langle a \rangle$, $b = a^n$ for some $n \in I$.

Since $a \in G = \langle b \rangle$, $a = b^m$ for some integer $m \in I$

$\therefore a = b^m$

$\therefore a = (a^n)^m$

$= a^{nm}$

NOW $a = a^{nm} \Rightarrow a^{nm-1} = e$

$\Rightarrow nm - 1 = 0$ (by (1))

$\Rightarrow nm = 1$

$\Rightarrow n = 1, m = 1$ or $n = -1, m = -1$

$\therefore b = a$ or a^{-1}

$\therefore G$ has exactly two generators a & a^{-1}.

TMS (INSTITUTE OF MATHEMATICAL SCIENCES)

→ Every subgroup of a cyclic group is cyclic.

proof: Let G be a cyclic group generated by 'a'.

$\therefore G = \langle a \rangle$

Let H be a subgroup of G.

If $H = G$ or $\{e\}$, then H is cyclic.

If H is a proper subgroup of G. then the elements of H are integral powers of 'a'.

If $a^s \in H$ then $a^{-s} \in H$

$\therefore$ H contains the elements which are +ve as well as −ve integral powers of a.

Let 'm' be the least +ve integer such that $a^m \in H$ then we have to prove that $H = \langle a^m \rangle$.

i.e, H is cyclic and is generated by a^m.

Let a^t be any arbitrary element of H. By division algorithm $\exists$ integers q & r such that

$t = mq + r$, $0 \le r < m$.

Now $a^m \in H \Rightarrow (a^m)^q \in H$. (By closure prop.)

$\Rightarrow a^{mq} \in H$

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

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

Also $a^t \in H$, $a^{-mq} \in H \Rightarrow a^t \cdot a^{-mq} \in H$

$\Rightarrow a^{t-mq} \in H$

$\Rightarrow a^r \in H$ $(\because r = t - mq)$

Now 'm' is the least +ve integer such that $a^m \in H$ and $0 \le r < m$.

$\therefore$ 'r' must be equal to zero.

$\therefore t = mq$

$\therefore a^t = a^{mq}$

$\Rightarrow a^t = (a^m)^q$.

$\therefore$ every element $a^t \in H$ is of the form $(a^m)^q$.

$\therefore$ H is a cyclic group and is generated by a^m.

Note: The converse of the above theorem need not be true.

i.e, the subgroup is cyclic, the group need not be cyclic.

Ex: W.K.T $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{R},+)$

Here $(\mathbb{Z},+)$ is a cyclic group generated by $+1$, and -1

But $(\mathbb{R},+)$ is not a cyclic group.
($\because$ it has no generators).

Theorem → If 'p' is a prime number then every group of order 'p' is a cyclic group.

i.e, a group of prime order is cyclic.

Proof: Let $p \geq 2$ be a prime number and G be a group such that $o(G) = p\ (\geq 2)$

Since the number of elements in G is atleast 2,

One of the elements of G will be different from the identity $e \in G$.

Let that be 'a'.

Let $\langle a \rangle$ be the cyclic subgroup of G generated by 'a'.

$\therefore a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \{e\}$.

Let $\langle a \rangle$ be of order h.

$\therefore$ By Lagrange's theorem h/p i.e, $\frac{p}{h}$.

But p is prime number.

$\therefore h = 1$ or $h = p$.

But $\langle a \rangle \neq \{e\}$ and hence $h = p$.

$\therefore o(\langle a \rangle) = p = o(G)$

i.e, $\langle a \rangle = G$.

which shows that G is a cyclic group.

Note [1]. we have by the above theorem if $o(G)=p$, (a prime number) then every element of G which is not an identity is a generator of G.
i.e, the number of generators of G having p elements is equal to $p-1$.

[2]. Every Group G of order less than 6 is abelian,
for:
we know that every group G of order less than or equal to 4 is abelian.
Also w.k.t every group of prime order is cyclic and every cyclic group is abelian.
If $o(G)=5$ then G is abelian.
i.e, the smallest non abelian group is of order 6.

[3]. The converse of the above theorem need not be true.
i.e, every cyclic group of order need not be a prime number.
Ex: 4^{th} roots of unity w.r.t x^n form a cyclic group and 4 is not a prime number.

Theorem If a finite group of order 'n' contains an element of order 'n'. then the group is cyclic.

proof: Let G be a finite group of order 'n'. i.e $o(G)=n$
Let $a \in G$ such that $o(a)=n$
i.e, $a^n=e$ where 'n' is the least +ve integer.
If H is a cyclic subgroup of G generated by 'a'.
i.e, if $H=\{a^r / r \in \mathbb{Z}\}$
then $o(H)=n$.
because the order of the generator 'a' of H is 'n'.
$\therefore$ H is a cyclic subgroup of G and $o(H)=n=o(G)$.

$\therefore H = G$ and G itself is a cyclic group with 'a' as a generator.

Note: Suppose G is a finite group of order 'n' and we are to determine whether G is cyclic or not. For this we find the orders of the elements of G and if $a \in G$ exists such that $o(a) = n$, then G will be a cyclic group with 'a' as a generator.

Theorem Every finite group of composite order possesses proper subgroups.

proof: Let G be a finite group of composite order mn where $m(\neq 1)$ and $n(\neq 1)$ are +ve integers.

(i) Let G be the cyclic group and generated by 'a'.

$\therefore G = \langle a \rangle$.

$\Rightarrow o(a) = o(G) = mn$.

$\Rightarrow a^{mn} = e$

$\Rightarrow (a^n)^m = e$

$\Rightarrow o(a^n) \leq m$.

Let $o(a^n) = p$ where $p < m$.

then $(a^n)^p = e \Rightarrow a^{np} = e$

But $p < m \Rightarrow np < nm$

$\therefore a^{np} = e$ where $np < mn$.

Since $o(a) = mn$, $a^{np} = e$ is not possible. $(a^m \neq e)$ unless $p = m$.

$\therefore o(a^n) = m$.

$\therefore H = \langle a^n \rangle$ is a cyclic subgroup of G and $o(H) = o(a^n)$.

$\therefore o(H) = m$.

Since $2 \leq m < mn$.

$\therefore H$ is a proper subgroup of G.

(ii) Let G be not cyclic group.
Then order of each element of G must be less than mn.
So there exists an element say b in G such that $2 \leq O(b) < mn$.
Then $H = \langle b \rangle$ is a proper subgroup of G.

Theorem If a cyclic group G is generated by an element 'a' of order 'n', then a^m is a generator of G iff the greatest common divisor of m and n is 1. i.e, m, n are relatively prime.

proof: Let $G = \langle a \rangle$ such that $O(a) = n$
i.e, $a^n = e$.
The group G contains exactly 'n' elements

(i) Let m be relatively prime to 'n'.
Now consider the cyclic subgroup $H = \langle a^m \rangle$ of G.
Clearly $H \subseteq G$ —— ①
Since m, n are relatively prime, there exist two integers x & y such that $mx + ny = 1$.

$$\therefore a = a^1$$
$$= a^{mx+ny}$$
$$= a^{mx} \cdot a^{ny}$$
$$= a^{mx} \cdot (a^n)^y$$
$$= a^{mx} e^y$$
$$= a^{mx}$$
$$= (a^m)^x$$
$$\therefore a = (a^m)^x$$

$\therefore$ Each integral exponent of 'a' will also be some integral exponent of a^m.
$\therefore G \subseteq H$ —— ②
$\therefore$ from ① & ② we have $H = G$
and a^m is a generator of G.

(ii) Let $G = \langle a^m \rangle$

Let the greatest common divisor of m and n be $d(\neq 1)$ i.e, $d > 1$.

Then $\frac{m}{d}, \frac{n}{d}$ must be integers.

Now $(a^m)^{\frac{n}{d}} = a^{\frac{mn}{d}}$

$= (a^n)^{\frac{m}{d}}$

$= e^{\frac{m}{d}}$

$= e$

$\therefore (a^m)^{\frac{n}{d}} = e$

$\Rightarrow o(a^m) \leq \frac{n}{d} < n$

$\Rightarrow o(a^m) < n$

$\therefore a^m$ cannot be generator of G. because $o(a^m) \neq o(G)$.

Hence d must be equal to 1.

$\therefore m$ is prime to n.

Theorem

If G is a finite cyclic group of order 'n' generated by 'a' then the subgroups of G are precisely the subgroups generated by a^m, where m divides n.

proof: Since G is a finite cyclic group of order 'n' generated by 'a', then a^m generates a cyclic sub group, say H, of G i.e $H = \langle a^m \rangle$.

since $o(G) = n = o(a)$.

$\therefore a^n = e$ where $e \in G$.

Since H is a subgroup of G, $e \in H$

i.e, $a^n \in H$.

If 'm' is the least +ve integer such that $a^m \in H$ then by division algorithm, $\exists$ +ve integers q & r such that $n = mq + r$; $0 \leq r < m$.

$\therefore a^n = a^{mq+r}$

$= a^{mq} \cdot a^r$

$= (a^m)^q \cdot a^r$.

But $a^m \in H \Rightarrow (a^m)^q \in H$

$\Rightarrow \bar{a}^{mq} \in H$

Now $a^n \in H$, $\bar{a}^{mq} \in H \Rightarrow a^{n-mq} \in H$

$\Rightarrow a^r \in H$.

But $0 < r < m$ and $a^r \in H$ is a contradiction to our assumption that m is the smallest +ve integer such that $a^m \in H$.

$\therefore r = 0$

$\therefore n = mq$

i.e, m divides n.

and $a^n = a^{mq}$

$= (a^m)^q \in H$

which means that a^m generates the cyclic subgroup H of G.

Ex: write down all the subgroups of a finite cyclic group of order 18, the cyclic group being generated by 'a'.

Soln: Let e be the identity element in G.

NOW G, {e} are trivial subgroups of G and generated by 'a' and $a^{18} = e$ respectively.

The other proper subgroups are precisely the subgroups generated by a^m where m divides 18.

Such m's are 2, 3, 6, 9.

$\therefore$ The subgroups are

$\langle a^2 \rangle = \{ a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18} = e \}$,

$\langle a^3 \rangle = \{ a^3, a^6, a^9, a^{12}, a^{15}, a^{18} = e \}$, $\{ a^6, a^{12}, a^{18} = e \} = \langle a^6 \rangle$

and $\{ a^9, a^{18} = e \} = \langle a^9 \rangle$.

Euler ϕ-function:

If n is any +ve integer, then Euler ϕ-function, denoted by $\phi(n)$ is defined as $\phi(1) = 1$,
$\phi(n)$ = number of +ve integers less than n and relatively prime to n, if $n > 1$.

Ex: (1) $\phi(4) = 2$, since 1, 3 are the +ve integers less than 4 and relatively prime to 4.

(2) $\phi(5) = 4$, since 1, 2, 3, 4 are the +ve integers less than 5 and relatively prime to 5.

(3) $\phi(6) = 2$, since 1, 5 are the +ve integers less than 6 and relatively prime to 6.

(4) $\phi(8) = 4$, since 1, 3, 5, 7 are the +ve integers less than 8 and relatively prime to 8.

(5) $\phi(p) = p-1$, if p is prime.

Note: [1]. The number of generators of a finite cyclic group of order 'n' is $\phi(n)$, where $\phi(n)$ is the Euler ϕ-function.

(or)

If $G = \langle a \rangle$ be a finite cyclic group of order 'n' then a^m is a generator of G iff $0 < m < n$ and $(m, n) = 1$

[2]. From number theory, if $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots p_k$ are all prime factors of n, then $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

Further if $n = p^\alpha$ where p is less than n and prime to n then $\phi(n) = p^\alpha\left(1-\frac{1}{p}\right)$.

Problems:

Find the generators of a cyclic group of order 8.

Sol^n: we have $G = \langle a \rangle$, $a^8 = e$.

All the generators of G are a^1, a^3, a^5, a^7.

i.e, $G = \langle a \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle$.

(∵ 1, 3, 5, 7 are +ve integers less than 8 and prime to 8.

Note: Let U_n denote the group of integers relatively prime to n under multiplication mod n.

→ Show that U_9 is cyclic group. what are all its generators?

Sol^n: we have $U_9 = \{1, 2, 4, 5, 7, 8\}$

Now $2^1 = 2$, $2^2 = 2 \times_9 2 = 4$, $2^3 = 2 \times_9 2 \times_9 2 = 8$

$2^4 = 16 = 7$, $2^5 = 5$, $2^6 = 1$

$\therefore U_9 = \langle 2 \rangle$

$\therefore U_9$ is a cyclic group. and $O(U_9) = 6$.

The +ve integers less than 6 and prime to 6 are 1, 5.

Hence all the generators of U_9 are $2^1, 2^5$.

i.e, 2, 5.

→ Show that U_{17} is a cyclic group. what are all its generators?

Sol^n: $U_{17} = \{1, 2, \ldots\ldots 16\}$

and $O(U_{17}) = 16$

All the +ve integers less than 16 and prime to 16 are 1, 3, 5, 7, 9, 11, 13, 15.

we can easily verify that $U_{17} = \langle 3 \rangle$.

i.e, every element of U_{17} is a power of 3.

All the generators of U_{17} are $3^1 = 3$, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$, $3^{15} = 6$.

Hence all the generators of U_{17} are,

$3, 5, 6, 7, 10, 11, 12, 14$.

→ Is U_8 a cyclic group?

Soln: Let $U_8 = \{1, 3, 5, 7\}$

$O(U_8) = 4$.

Since $3^1 = 3$, $3^2 = 1$, $3^3 = 3$, $3^4 = 1$, $3^5 = 1$ etc.

$\therefore$ 3 is not generator of U_8.

Since $5^1 = 5$, $5^2 = 1$, $5^3 = 5$ etc.

$\therefore$ 5 is not generator of U_8.

Similarly 7 is not generator of U_8.

$\therefore$ U_8 is not cyclic.

→ Find the number of generators of cyclic groups of orders 5, 6, 8, 12.

Soln: $O(G) = 5$,

the number of generators of $G = \phi(5)$

$= 5(1-\frac{1}{5}) = 4$.

$O(G) = 6$.

the number of generators of $G = \phi(6)$

$= 6(1-\frac{1}{2})(1-\frac{1}{3})$

$= 6(\frac{1}{2})(\frac{2}{3})$

$= 2$ ($\because 6 = 2^1 \times 3^1$ i.e, 2, 3 are prime factors of 6.)

$O(G) = 8$.

the number of generators of $G = \phi(8)$

$= 2^3(1-\frac{1}{2}) = 4$ ($\because$ 2 is the only prime factor of 8)

$O(G) = 12$.

the number of generators of $G = \phi(12)$

$= 12(1-\frac{1}{2})(1-\frac{1}{3})$

$= 4$

($\because 12 = 4 \times 3 = 2^2 \times 3^1$)