Cyclic Group

A group G is called cyclic if there is an element a in G such that $G = \{a^n \mid n \in \mathbb{Z}\}$

Such an element a is called the generator of G.

Notation: $G = \langle a \rangle$.

Examples: $\mathbb{Z}_6$, $U(10)$, $\mathbb{Z}$

Examples: $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

generators 1 and 7

3 and 5 are also generators.

$(3)^1 = 3$

$(3)^2 = 3 +_8 3 = 6$

$3^3 = 3 +_8 3 +_8 3 = 1$

$3^4 = 1 +_8 3 = 4$

$3^5 = 4 +_8 3 = 7$

$3^6 = 7 +_8 3 = 2$

$3^7 = 2 +_8 3 = 5$

$3^8 = 5 +_8 3 = 0$.

$\langle 3 \rangle = \{3^n \mid n \in \mathbb{Z}\}$

$= \{\ldots \bar{3}^3, \bar{3}^2, \bar{3}^1, 3^0, 3^1, 3^2, 3^3, 3^4, \ldots\}$

$= \{3, 6, 1, 4, 7, 2, 5, 0\}$

$= \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8$

This implies 3 is the generator of $\mathbb{Z}_8$.

Note: ① If a is the generator of a group G, then a^{-1} is also the generator of G.

② 1 is always the generator of $\mathbb{Z}_n$.

$(n-1)$ is always the generator of $\mathbb{Z}_n$.

In $\mathbb{Z}_n$, $(1)^{-1} = (n-1)$

$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$

1 and $(n-1)$ are always the generators of $\mathbb{Z}_n$.

③ order of an element $a \in G$ is the smallest positive integer n such that $a^n = e$

$|a| = n$ and $a^k = e$ for some $k > 0$.

then $k \geq n$.

$a^0 = e$

Thm Let G be a group and $a \in G$. If a has infinite order, then all distinct powers of a are distinct group elements.

If a has finite order (say n), then

$\langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$ and

$a^i = a^j$ iff n divides $i-j$.

Proof: Let $a \in G$ and a has infinite order.

The powers of a are, $a, a^2, a^3, \ldots, a^i, \ldots a^j, \ldots$

Suppose $a^i = a^j$ for some $i < j$

$\Rightarrow a^j = a^i$

$\Rightarrow a^j \cdot \bar{a}^i = a^i \cdot \bar{a}^i$

$\Rightarrow a^{j-i} = e$. $\left[\because i<j \Rightarrow j-i>0\right]$

$\Rightarrow |a| \leq j-i$

This contradicts the fact that a has infinite order.

$\therefore a^i \neq a^j$ for $(i \neq j)$.

Thus, all distinct powers of a are distinct group elements.

Now, assume that $|a| = n$.

We will prove that $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$
$= \{a^0, a^1, a^2, a^3, \ldots\}$
$\bar{a}^3, \bar{a}^2, \bar{a}^1, \ldots\}$

Now the elements $e, a, a^2, \ldots a^{n-1}$ are distinct.

Suppose $a^i = a^j$ for some

Suppose $a^i = a^j$ for some $0 \le i < j \le n-1$

$\Rightarrow a^j = a^i$

$\Rightarrow a^{j-i} = e$

$\Rightarrow |a| \le j-i < n$ $\left[\because i<j \Rightarrow j-i>0\right]$

This contradicts the fact that $|a| = n$.

Now, suppose that a^k is an arbitrary member of $\langle a \rangle$.

By division algorithm, there exists integers q and r such that

$k = nq + r$, where $0 \le r \le n-1$

Now, $a^k = a^{nq+r} = a^{nq} \cdot a^r$

$= (a^n)^q \cdot a^r = e^q \cdot a^r$ $(\because |a| = n \Rightarrow a^n = e)$

$= e \cdot a^r = a^r \in \{e, a, a^2, \ldots, a^{n-1}\}$

$\therefore a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$ for all $k \in \mathbb{Z}$.

$\Rightarrow \langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$.

Next, Assume that $a^i = a^j$

To Prove: n divides $(i-j)$.

Now, $a^i = a^j \Rightarrow a^i a^{-j} = a^j a^{-j}$

$\Rightarrow a^{i-j} = e$ ——— (1)

By division algorithm, $\exists$ integers q & r such that

$i-j = qn + r$, where $0 \le r \le n-1$.

——— (2)

Now $a^{i-j} = a^{qn+r}$

$\Rightarrow e = a^{qn} \cdot a^r$ [from eqn (1)]

$\Rightarrow (a^n)^q \cdot a^r = e$

$\Rightarrow e^q \cdot a^r = e$

$\Rightarrow a^r = e$, where $0 \le r \le n-1$

$\Rightarrow r = 0$ [$\because |a| = n$]

Now, from eqn (2), $i-j = qn + 0$

$\Rightarrow i-j = qn$

$\Rightarrow n$ divides $(i-j)$.

Conversely (⊆) suppose that n divides $(i-j)$.

To prove $a^i = a^j$.

Suppose n divides $(i-j) \Rightarrow i-j = qn$

Now, $a^{i-j} = a^{qn} = (a^n)^q$ where $q \in \mathbb{Z}$.

$\Rightarrow a^{i-j} = e^q = e$

$\Rightarrow a^i = a^j$

Corollary:-

Let G be a group and a be an element of order n in G. If $a^k = e$, then n divides k.

Proof: $a^k = e$ & $|a| = n$.

either $k=0$, or $k \geq n$

if $k=0$, then n divides k.

If $k \geq n$, then by division algorithm

$\exists$ q & r such that

$k = qn + r, \quad 0 \leq r \leq n-1$

$a^k = e \Rightarrow a^r = e$, where $0 \leq r \leq n-1$

$\Rightarrow r = 0.$

$\therefore k = qn$

$\Rightarrow$ n divides k.

Generators of Cyclic Groups:

Th^m 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: First let $G = \langle a^k \rangle$

$\Rightarrow$ a^k is the generator of G

$\therefore$ $G = \langle a \rangle$ & $|a| = n \Rightarrow |G| = n$

TS $\gcd(k, n) = 1$

Now suppose that $\gcd(k, n) = d > 1$. ——— (1)

$\therefore$ We can write $k = td$ and $n = sd$

where $1 \leq t < k$

and $1 \leq s < n$ ——— (2)

$k = td$

$n = sd$

$\Rightarrow n = 1$

Now $(a^k)^s = (a^{td})^s = a^{tds}$

$= (a^{sd})^t = (a^n)^t$

$= e^t = e$

$\Rightarrow |a^k| \leq s < n = |G|$

$\therefore |a^k| < |G|$

$\Rightarrow a^k$ is not the generator of G

$\Rightarrow G \neq \langle a^k \rangle$

Note: Let G be a group and a be the generator of G, then $|G| = |a|$.

This is a contradiction as we have assumed that $G = \langle a^k \rangle$

$\therefore \gcd(k, n) = 1$

Conversely ($\Leftarrow$) Let $\gcd(k, n) = 1$

TS $G = \langle a^k \rangle$.

$\because \gcd(k, n) = 1 \Rightarrow$ there exists integers u and v such that

$ku + nv = 1$ ——— (3)

Now $a = a^1 = a^{ku+nv} = a^{ku} \cdot a^{nv}$

$\Rightarrow a = a^{ku} \cdot (a^n)^v$ $\quad \because |a| = n$

$\Rightarrow a = a^{ku} \cdot u$

$\Rightarrow a = (a^k)$.

$\Rightarrow a \in \langle a^k \rangle$

$\Rightarrow \langle a \rangle \subseteq \langle a^k \rangle$ ——— (4)

Now, $a^k \in \langle a \rangle$ for every value of k.

$\Rightarrow \langle a^k \rangle \subseteq \langle a \rangle$ ——— (5)

from eqn (4) & (5),

$\langle a \rangle = \langle a^k \rangle$

$\Rightarrow G = \langle a^k \rangle$

$A \subseteq B$
& $B \subseteq A$
$\Rightarrow A = B$

$G = \langle a^k \rangle$
$G = \langle a \rangle$
$\therefore \langle a \rangle = \langle a^k \rangle$

$a \in H$
$a^2 \in H$
$a^3 \in H$
$\vdots$
$a^{-1} \in H$
$\vdots$

Corollary:

Generators of $\mathbb{Z}_n$

An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(k, n) = 1$

Proof: 1 is always the generator of $\mathbb{Z}_n$

$\therefore \mathbb{Z}_n = \langle 1 \rangle$.

By previous thm

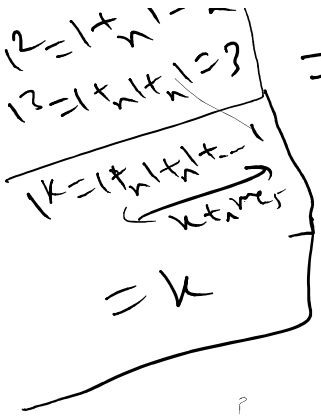
$G = \langle 1^k \rangle$ iff $\gcd(k, n) = 1$

$\Rightarrow 1^k$ is the generator of $\mathbb{Z}_n$ iff $\gcd(k, n) = 1$

$\Rightarrow k$ is the generate of $\mathbb{Z}_n$ iff $\gcd(k, n) = 1$.

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$1^1 = 1$
$1^2 = 1 + n\,1 = 2$
$1^3 = 1 + n\,1 + n\,1 = 3$



$\Rightarrow$ k is the generate of $\mathbb{Z}_n$ iff $\gcd(k,n)=1$.