Cyclic groups

Dr.E.Geetha
Assistant Professor of Mathematics
SCSVMV

Aim

- Cyclic groups
- Order of Cyclic groups
- Generators of cyclic groups
- Euler Phi function

Prerequisities

- Group and its order
- Subgroup

Learning outcome

Students can be able to

- Identify cyclic groups and its Order
- Find the Generators of cyclic groups
- With the use of Euler Phi function, they came know to find the generators of cyclic groups.

Definition: Cyclic groups

- A cyclic group is a group which can be generated by one of its elements.
- That is, for some a in G,
  G = $\{a^n$ | n is an element of Z}

Or, in addition notation,
G = { na | n is an element of Z }

This element a (Which need not be unique) is called a generator of G.

Alternatively, we may write G = < a >.

Example:-

(i) Let G={1, -1, i, -i}, then {G,x} be a group, where e=1 is the multiplicative ***identity*** element.

Clearly i and -i are the two generators of G,

Since $(i)^1=i$, $(i)^2=-1$, $(i)^3=-i$, and $(i)^4=1$.

$(-i)^1=-i$, $(-i)^2=-1$, $(-i)^3=i$, and $(-i)^4=1$

Hence {G,x} is a ***cyclic group.***

(ii) Let $G=\{1, w, w^2\}$, then {G,x} be a group , where $w^3=1$ and e=1 is the multiplicative **identity** element .

Clearly w and w^2 are the two generators of G

Since $(w)^1=w$, $(w)^2=w^2$, $(w)^3=1$

$(w^2)^1=w^2$, $(w^2)^2=w^4=w$ $(w^2)^3=w^6=1$

Hence {G,x} is a ***cyclic group.***

(iii) Let $G=\{a, a^2, a^3, \ldots a^n\}$, then $\{G,x\}$ be a group, where $a^n=e$, and 'e' is multiplicative identity element.

Clearly a is the only generator of G

Since $(a)^1=a$, $(a)^2=a^2$, $(a)^3=a^3$, $\ldots\ldots\ldots(a)^n=a^n=e$.

Hence $\{G,x\}$ is a ***cyclic group.***

Definition: Order of a cyclic group

If a generator g has order n, $G = \langle g \rangle$ is **cyclic of order** n. If a generator g has infinite order, $G = \langle g \rangle$ is **infinite cyclic**.

Example. (The integers and the integers mod n are cyclic) Show that $\mathbb{Z}$ and $\mathbb{Z}_n$ for $n > 0$ are cyclic.

$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of 1 (or of -1). For instance, $117 = 117 \cdot 1$. (Remember that "$117 \cdot 1$" is really shorthand for $1 + 1 + \cdots + 1$ — 1 added to itself 117 times.)

In fact, it is the only infinite cyclic group up to **isomorphism**.

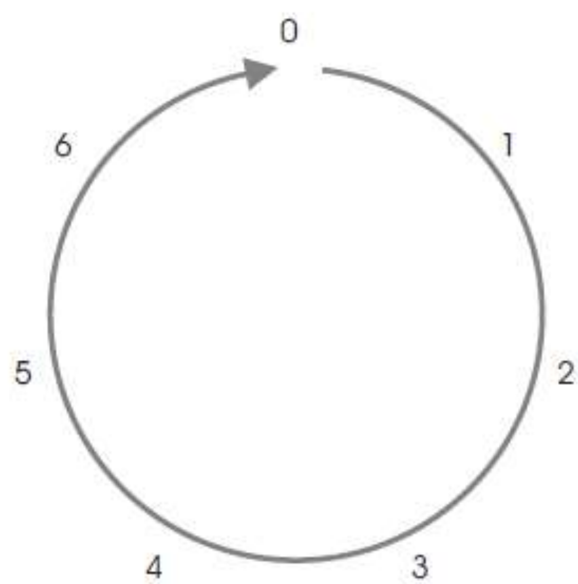
Notice that a cyclic group can have more than one generator.

If n is a positive integer, $\mathbb{Z}_n$ is a cyclic group of order n generated by 1.

For example, 1 generates $\mathbb{Z}_7$, since

$$
\begin{aligned}
1+1&=2\\
1+1+1&=3\\
1+1+1+1&=4\\
1+1+1+1+1&=5\\
1+1+1+1+1+1&=6\\
1+1+1+1+1+1+1&=0
\end{aligned}
$$

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.



a cyclic group of order 7

Notice that 3 also generates $\mathbb{Z}_7$:

$$
\begin{aligned}
3+3&=6\\
3+3+3&=2\\
3+3+3+3&=5\\
3+3+3+3+3&=1\\
3+3+3+3+3+3&=4\\
3+3+3+3+3+3+3&=0
\end{aligned}
$$

The "same" group can be written using multiplicative notation this way:

$$\mathbb{Z}_7 = \{1, a, a^2, a^3, a^4, a^5, a^6\}.$$

In this form, a is a generator of $\mathbb{Z}_7$.
It turns out that in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group.
On the other hand, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate. □

Lemma. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order n. Then the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct.

Proof. Since g has order n, g, g^2, $\ldots g^{n-1}$ are all different from 1.

Now I'll show that the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. Suppose $g^i = g^j$ where $0 \leq j < i < n$. Then $0 < i - j < n$ and $g^{i-j} = 1$, contrary to the preceding observation.

Therefore, the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. $\square$

Lemma. Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.

Proof. One of m, n is larger — suppose without loss of generality that $m > n$. I want to show that $g^m \neq g^n$; suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$. $\square$

Lemma. Let G be a group, and let $g \in G$ have order m. Then $g^n = 1$ if and only if m divides n.

Proof. If m divides n, then $n = mq$ for some q, so $g^n = (g^m)^q = 1$.
Conversely, suppose that $g^n = 1$. By the Division Algorithm,

$$n = mq + r \quad \text{where} \quad 0 \leq r < m.$$

Hence,

$$g^n = g^{mq+r} = (g^m)^q g^r \quad \text{so} \quad 1 = g^r.$$

Since m is the smallest positive power of g which equals 1, and since $r < m$, this is only possible if $r = 0$. Therefore, $n = qm$, which means that m divides n. □

Example. (The order of an element) Suppose an element g in a group G satisfies $g^{45} = 1$. What are the possible values for the order of g?

The order of g must be a divisor of 45. Thus, the order could be

$$1, \quad 3, \quad 5, \quad 9, \quad 15, \quad \text{or} \quad 45.$$

And the order is certainly not (say) 7, since 7 doesn't divide 45. $\square$

Proposition. Let $G = \langle g \rangle$ be a cyclic group of order n, and let $m < n$. Then g^m has order $\dfrac{n}{(m,n)}$.

Remark. Note that the order of g^m (the element) is the same as the order of $\langle g^m \rangle$ (the subgroup).

Proof. Since (m,n) divides m, it follows that $\dfrac{m}{(m,n)}$ is an integer. Therefore, n divides $\dfrac{mn}{(m,n)}$, and by the last lemma,

$$(g^m)^{\frac{n}{(m,n)}} = 1.$$

Now suppose that $(g^m)^k = 1$. By the preceding lemma, n divides mk, so

$$\frac{n}{(m,n)} \,\Big|\, k \cdot \frac{m}{(m,n)}.$$

However, $\left(\dfrac{n}{(m,n)}, \dfrac{m}{(m,n)}\right) = 1$, so $\dfrac{n}{(m,n)}$ divides k. Thus, $\dfrac{n}{(m,n)}$ divides any power of g^m which is 1, so it is the order of g^m. $\square$

In terms of $\mathbb{Z}_n$, this result says that $m \in \mathbb{Z}_n$ has order $\dfrac{n}{(m,n)}$.

Example. **(Finding the order of an element)** Find the order of the element a^{32} in the cyclic group $G = \{1, a, a^2, \ldots a^{37}\}$. (Thus, G is cyclic of order 38 with generator a.)

In the notation of the Proposition, $n = 38$ and $m = 32$. Since $(38, 32) = 2$, it follows that a^{32} has order $\frac{38}{2} = 19$. □

Corollary. The generators of $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ are the elements of $\{0, 1, 2, \ldots, n-1\}$ which are relatively prime to n.

Proof. If $m \in \{0, 1, 2, \ldots, n-1\}$ is a generator, its order is n. The Proposition says its order is $\dfrac{n}{(m, n)}$. Therefore, $n = \dfrac{n}{(m, n)}$, so $(m, n) = 1$.

Conversely, if $(m, n) = 1$, then the order of m is

$$\frac{n}{(m, n)} = \frac{n}{1} = n.$$

Therefore, m is a generator of $\mathbb{Z}_n$. $\square$

Example. (Finding the generators of a cyclic group) List the generators of:

(a) $\mathbb{Z}_{12}$.

(b) $\mathbb{Z}_p$, where p is prime.

(a) The generators of $\mathbb{Z}_{12}$ are 1, 5, 7, and 11. These are the elements of $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ which are relatively prime to 12. □
(b) If p is prime, the generators of $\mathbb{Z}_p$ are 1, 2, ..., $p - 1$. □

Example. (a) List the generators of $\mathbb{Z}_9$.

(b) List the elements of the subgroup $\langle 3 \rangle$ of $\mathbb{Z}_{27}$.

(c) List the generators of the subgroup $\langle 3 \rangle$ of $\mathbb{Z}_{27}$.

(a) The generators are the elements relatively prime to 9, namely 1, 2, 4, 5, 7, and 8. $\square$

(b)

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}. \quad \square$$

(c) $\langle 3 \rangle$ is cyclic of order 9, so its generators are the elements corresponding to the generators 1, 2, 4, 5, 7, and 8 of $\mathbb{Z}_9$. Since $27 = 3 \cdot 9$, I can just multiply these generators by 3.

Thus, the generators of $\langle 3 \rangle$ are 3, 6, 12, 15, 21, and 24. $\square$

Properties of Cyclic groups

(i) Every cyclic group is abelian

(ii) If a is a generator of a cyclic group {G,*}, then a^{-1} is also a generator of {G,*}.

Proof of (i)

Let {G,*} be a cyclic group with 'a' in G is a generator.

We have to prove G is abelian,

i.e to prove $b*c=c*b$, for all b,c in G

Since b lies in G and 'a' is generator of G, therefore $b=a^m$----(1), for some integer m.

Since c lies in G and 'a' is generator of G, therefore $c=a^n$-----(2), for some integer n.

Now L.H.S=$b*c$

$=a^m*a^n$

$=a*a*a*......*a*a*a.....*a$

$=a^{m+n}$

$=a^{n+m}$ (since n,m are integers, therefore n+m=m+n)

$=a^n*a^m$

$=c*b$

L.H.S=R.H.S

Hence the proof.

Proof of (ii)

Let 'a' is generator of a cyclic group {G,*}

We have to prove 'a^{-1}' is also a generator of {G,*}

Let 'b' any element in G and 'a' is generator of G, therefore $b=a^m$, for some integer m.

i.e $b=(a^{-1})^{-m}$ for some integer -m

Hence a^{-1} is also a generator of G.

Properties of cyclic groups

- Criterion for $a^i = a^j$

  For $|a| = n$, $a^i = a^j$ Iff n divides (i – j)

  (alternatively, if i = j mod n)

  Or in addition notation, ia = ja iff i = j mod n

  Corollaries:

  1. $|a| = |\langle a \rangle|$, that is, the order of an element is equal to the order of the cyclic group generated by that element.

  2. If $a^k = e$ then the order of a divides k

- For $|a| = n$,

$$< a^k > = < a^{\gcd(n,k)} > \; and \; |a^k| = n / \gcd(n,k)$$

Corollary:

1. Let $|a| = n$. then $< a^i > = < a^j >$ iff gcd (n, i) = gcd (n, j)

2. In any cyclic group G = <a> with order n, the generators are a^k for each k relatively prime to n.

Fundamental theorem of Cyclic groups

- Let G = <a> be a cyclic group of order n. Then

1. Every subgroup of a cyclic group is also cyclic.
2. The order of each subgroup divides the order of the group.
3. For each divisor k of n, there is exactly one subgroup of order k, that is $< a^{n/k} >$

Number of elements of each order in a cyclic group

- Let G be a cyclic group of order n.

Then, if d is a positive divisor of n, then the number of elements of order d is $\varphi(d)$ where φ

is the Euler Phi function.

$\varphi(d)$ is defined as the number of positive integers less than d and relatively prime to d

The First few values of $\varphi(d)$ are:

d	1	2	3	4	5	6	7	8	9
$\varphi(d)$	1	1	2	2	4	2	6	4	6

Thank you