Cyclic Groups

Def^n (Cyclic Group): A group H is a cyclic group if $\exists$ an element $x \in H$ such that $H = \{x^n : n \in \mathbb{Z}\}$

i.e. every element of H can be expressed as some integral power of x;

$\rightarrow$ x is called generator of H

$$H = \{ \dots, x^{-3}, x^{-2}, x^{-1}, x^0, x^1, x^2, x^3, \dots \}$$

If operation of the group H is addition $(+)$, then

$$H = [x] = \{ \dots, -3x, -2x, -x, 0, x, 2x, 3x, \dots \}$$

Ex 1 $H = \{1, -1, i, -i\}$

$H = [i]$ ← generator

$i^0 = 1$
$i^1 = i$
$i^2 = -1$
$i^3 = -i$

Ex 2: Let $G = D_{2n} = \{ rs : r^n = s^2 = 1, rs = sr^{-1} \}$, $n \geq 3$ and let H be the subgroup of all rotations of the n-gon. Thus $H = [r]$ and the distinct elements of H are $1, r, r^2, \dots, r^{n-1}$

Proposition 2: If $H = \langle x \rangle$, then $|H| = |x|$. More specifically

(i) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H, and

(ii) if $|H| = \infty$, then $x^n \neq 1$ $\forall$ $n \neq 0$ and $x^a \neq x^b$ $\forall$ $a \neq b$ in $\mathbb{Z}$.

Proposition 3: Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$. In particular if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

Proposition 6: Let $H = \langle x \rangle$.

i) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ iff $a = \pm 1$.

ii) Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ iff $(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$ [where ϕ is Euler's ϕ function).

Example: Proposition 6 tells precisely which residue classes mod n generate $\mathbb{Z}/n\mathbb{Z}$; namely $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ iff $(a, n) = 1$.

For instance $\bar{1}, \bar{5}, \bar{7}$ and $\overline{11}$ are the generators of $\mathbb{Z}/12\mathbb{Z}$ and $\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = 2^1 \cdot (3-1) = 4$.

Theorem 7: Let $H = \langle x \rangle$ be a cyclic group.

1) Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

2) If $|H| = \infty$, then for any ~~element~~ distinct non-negative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the non-trivial subgroups of H correspond bijectively with the integers $1, 2, 3, \ldots$

3) If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$.

Example 1: There exists only two elements 1 and $-1 \in \mathbb{Z}$ such that every integer in $(\mathbb{Z}, +)$ either can be generated by 1 or -1, i.e. $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

Example 2: Consider the group $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Observe that

$\bar{1}$, $\bar{2} = \bar{1} \oplus_3 \bar{1}$, $\bar{0} = \bar{1} \oplus_3 \bar{1} \oplus_3 \bar{1}$

$\bar{2}$, $\bar{1} = \bar{2} \oplus_3 \bar{2}$, $\bar{0} = \bar{2} \oplus_3 \bar{2} \oplus_3 \bar{2}$

Thus every element of $\mathbb{Z}_3$ can be written in terms of $\bar{1}$ or $\bar{2}$. This type of group is called cyclic group and $\bar{1}$ and $\bar{2}$ are called the generators of the group.

Ex 3: $\mathbb{Z}_n$ is a cyclic group, as

$$\bar{n} = \bar{1} \oplus_n \cdots \oplus_n \bar{1} \quad (n\text{-times})$$

Thus $\bar{1}$ is called the generator of $\mathbb{Z}_n$.

Imp

* Note 1: $\bar{i}$ is generator of $\mathbb{Z}_n$ iff $\gcd(i, n) = 1$.

Imp

Ex 4: Find all generators of $\mathbb{Z}_{15}$.

Sol^n: Since

$$\gcd(1,15) = \gcd(2,15) = \gcd(4,15) = \gcd(7,15) = \gcd(8,15)$$
$$= \gcd(11,15) = \gcd(13,15) = \gcd(14,15) = 1$$

Thus $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}$ are generators of $\mathbb{Z}_{15}$.

Imp Note 2: Let $(G, *)$ be a finite group. Then $\exists$ an element $a \in G$ with $o(a) = o(G)$ iff G is cyclic.
Also, if $o(a) = o(G)$, then "a" is a generator of G.

Ex 5: Prove that Q_8 is not cyclic.

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

Sol^n Observe that in Q_8

$o(1) = 1, \quad o(-1) = 2, \quad o(\pm i) = o(\pm j) = o(\pm k) = 4$

Thus there is no element in Q_8 whose order is 8.

Product of Groups

Let $(G, *)$ and (H, o) be two groups with identity e and e' respectively. Consider the cartesian product of G and H

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

Let us define a binary operation on

$$(g, h) \cdot (g_1, h_1) = (g * g_1, h \, o \, h_1).$$

Observe that:

1) $((g, h) \cdot (g_1, h_1)) \cdot (g_2, h_2) = (g, h) \cdot ((g_1, h_1) \cdot (g_2, h_2)) \; \forall$
$(g, h), (g_1, h_1), (g_2, h_2) \in G \times H$

2) $\forall (g, h) \in G \times H$
$(g, h) \cdot (e, e') = (g, h) = (e, e') \cdot (g, h)$

3) Inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1})

$\therefore$ $G \times H$ forms a group.

Examples:

1) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$

Here $(\bar{0},\bar{0})$ is the identity element, inverse of $(\bar{1},\bar{0})$ is $(\bar{1},\bar{0})$, inverse of $(\bar{0},\bar{1})$ is $(\bar{0},\bar{1})$ and inverse of $(\bar{1},\bar{1})$ is $(\bar{1},\bar{1})$.

$$(\bar{1},\bar{0})\cdot(\bar{1},\bar{0}) = (\bar{1}\oplus_2\bar{1}, \bar{0}\oplus_2\bar{0}) = (\bar{0},\bar{0})$$

$$(\bar{1},\bar{1})\cdot(\bar{1},\bar{1}) = (\bar{1}\oplus_2\bar{1}, \bar{1}\oplus_2\bar{1}) = (\bar{0},\bar{0})$$

2) $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2})\}$

$$(\bar{0},\bar{1})\cdot(\bar{0},\bar{2}) = (\bar{0}\oplus_2\bar{0}, \bar{1}\oplus_3\bar{2}) = (\bar{0},\bar{0})$$

$$(\bar{1},\bar{1})\cdot(\bar{1},\bar{2}) = (\bar{1}\oplus_2\bar{1}, \bar{1}\oplus_3\bar{2}) = (\bar{0},\bar{0})$$

$$(\bar{1},\bar{0})\cdot(\bar{1},\bar{0}) = (\bar{1}\oplus_2\bar{1}, \bar{0}\oplus_3\bar{0}) = (\bar{0},\bar{0})$$

Here inverse of $(\bar{0},\bar{1})$ is $(\bar{0},\bar{2})$, inverse of $(\bar{1},\bar{0})$ is $(\bar{1},\bar{0})$, inverse of $(\bar{1},\bar{1})$ is $(\bar{1},\bar{2})$.

Note: $o(g,h) = \text{l.c.m}(o(g), o(h))$

Ex 3) Find order of each element of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$$o((\bar{0},\bar{0})) = 1$$

$$o((\bar{0},\bar{1})) = \text{l.c.m}(o(\bar{0}), o(\bar{1})) = \text{l.c.m}(1,2) = 2$$

$$o((\bar{1},\bar{0})) = \text{l.c.m}(o(\bar{1}), o(\bar{0})) = \text{l.c.m}(2,1) = 2$$

$$o((\bar{1},\bar{1})) = \text{l.c.m}(o(\bar{1}), o(\bar{1})) = \text{l.c.m}(2,2) = 2$$

Art 2.3 Exercise.

Imp Que1: Find all subgroups of $\mathbb{Z}_{45} = \langle x \rangle$, giving a generator for each.

Sol^n: The subgroups are generated by x^d where d divides 45.

divisors of 45 are $1, 3, 5, 9, 15, 45$

$$\mathbb{Z}_{45} = \langle \bar{1} \rangle$$

Subgroups $\langle \bar{1} \rangle$, $\langle \bar{3} \rangle$, $\langle \bar{5} \rangle$, $\langle \bar{9} \rangle$, $\langle \overline{15} \rangle$, $\langle \overline{45} \rangle$

$\langle \bar{1} \rangle \downarrow \mathbb{Z}_{45}$ $\quad$ $\langle \overline{45} \rangle \downarrow \langle \bar{0} \rangle$

$$\mathbb{Z}_{45} = \langle \bar{1} \rangle > \langle \bar{3} \rangle, \langle \bar{5} \rangle, \langle \bar{9} \rangle, \langle \overline{15} \rangle ; \langle \bar{0} \rangle$$

$$\langle \bar{3} \rangle > \langle \bar{9} \rangle, \langle \overline{15} \rangle, \langle \bar{0} \rangle$$

$$\langle \bar{5} \rangle > \langle \overline{15} \rangle, \langle \bar{0} \rangle$$

$$\langle \bar{9} \rangle > \langle \bar{0} \rangle$$

$$\langle \overline{15} \rangle > \langle \bar{0} \rangle$$

Imp

Que 3: Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Sol^n: The generators are those residue classes which are relatively prime to 48. Therefore the generators are $\bar{1}, \bar{5}, \bar{7}$, $\overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}, \overline{37}, \overline{41}$, $\overline{43}$ and $\overline{47}$.

Que 10: What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all the elements and their orders in $\langle \overline{30} \rangle$.

Sol^n: We know that

If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{(n, a)}$

Now, we have $|\bar{1}| = 54$

we can write.

$$\overline{30} = 30 \cdot \bar{1}$$

$$|\underset{a}{30} \cdot \bar{1}| = \frac{\overset{n}{54}}{\gcd(54, 30)} = \frac{54}{6} = 9$$

$\therefore \quad |\overline{30}| = 9$

Then $\langle \overline{30} \rangle = \{ \bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48} \}$

Imp.

Que 12 Prove that the following groups are not cyclic:

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$$

$$\therefore \quad o(\mathbb{Z}_2 \times \mathbb{Z}_2) = 4$$

Now $o((\bar{0},\bar{0})) = 1$

$$o((\bar{0},\bar{1})) = \text{l.c.m}(o(\bar{0}), o(\bar{1})) = \text{l.c.m}(1,2) = 2$$

$$o((\bar{1},\bar{0})) = \text{l.c.m}(o(\bar{1}), o(\bar{0})) = \text{l.c.m}(2,1) = 2$$

$$o((\bar{1},\bar{1})) = \text{l.c.m}(o(\bar{1}), o(\bar{1})) = \text{l.c.m}(2,2) = 2$$

As, there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ whose order 4,

hence $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Imp

Que: Check whether the group $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus_2 \times \oplus_3)$ is Cyclic or not.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2})\}$$

where $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ is a group under addition modulo 2.

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ is a group under addition modulo 3.

We can find an element $(\bar{1},\bar{1}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ such that

$(\bar{1},\bar{1})^2 = (\bar{1},\bar{1}) + (\bar{1},\bar{1}) = (\bar{0},\bar{2})$

$(\bar{1},\bar{1})^3 = (\bar{0},\bar{2}) + (\bar{1},\bar{1}) = (\bar{1},\bar{0})$

$(\bar{1},\bar{1})^4 = (\bar{1},\bar{0}) + (\bar{1},\bar{1}) = (\bar{0},\bar{1})$

$(\bar{1},\bar{1})^5 = (\bar{0},\bar{1}) + (\bar{1},\bar{1}) = (\bar{1},\bar{2})$

$(\bar{1},\bar{1})^6 = (\bar{1},\bar{2}) + (\bar{1},\bar{1}) = (\bar{0},\bar{0})$

$\because (\bar{1},\bar{1})$ generates all the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$, i.e. $\langle(\bar{1},\bar{1})\rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$

Hence $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

V.V Imp

Que : Find the subgroups of $\mathbb{Z}_{50}$.

Solⁿ : The divisors of 50 are 1, 2, 5, 10, 25, 50.

Hence subgroups of $\mathbb{Z}_{50}$ are

$$\langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{5} \rangle, \langle \overline{10} \rangle, \langle \overline{25} \rangle, \langle \overline{50} \rangle$$

$\langle \bar{1} \rangle \downarrow \mathbb{Z}_{50}$

$\langle \overline{50} \rangle \downarrow \langle \bar{0} \rangle$

Ans.

Art 2.5 The Lattice of subgroups of a group

Here we describe a graph associated with a group which depicts the relationship among its subgroups. This graph is called the lattice of subgroups of the group.

Examples:

(i) $\mathbb{Z}/4\mathbb{Z}$ divisors $1, 2, 4$

subgroups $\langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{4} \rangle$

$$\begin{array}{ccc} \langle \bar{1} \rangle & & \langle \bar{4} \rangle \\ \downarrow & & \downarrow \\ \mathbb{Z}_4 & & \langle \bar{0} \rangle \end{array}$$

$$\begin{array}{c} \mathbb{Z}_4 = \langle \bar{1} \rangle \\ | \\ \langle \bar{2} \rangle \\ | \\ \langle \bar{4} \rangle = \langle \bar{0} \rangle \end{array}$$

Lattice of subgroup

(ii) $\mathbb{Z}/6\mathbb{Z}$ divisors $1, 2, 3, 6$

subgroups $\langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{3} \rangle, \langle \bar{6} \rangle$

$$\begin{array}{ccc} \langle \bar{1} \rangle & & \langle \bar{6} \rangle \\ \downarrow & & \downarrow \\ \mathbb{Z}_6 & & \langle \bar{0} \rangle \end{array}$$

$$\begin{tikzcd} & \mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle \arrow[dl, dash] \arrow[dr, dash] & \\ \langle \bar{2} \rangle \arrow[dr, dash] & & \langle \bar{3} \rangle \arrow[dl, dash] \\ & \langle \bar{6} \rangle = \langle \bar{0} \rangle & \end{tikzcd}$$

V.V Imp

(3) The lattice of S_3

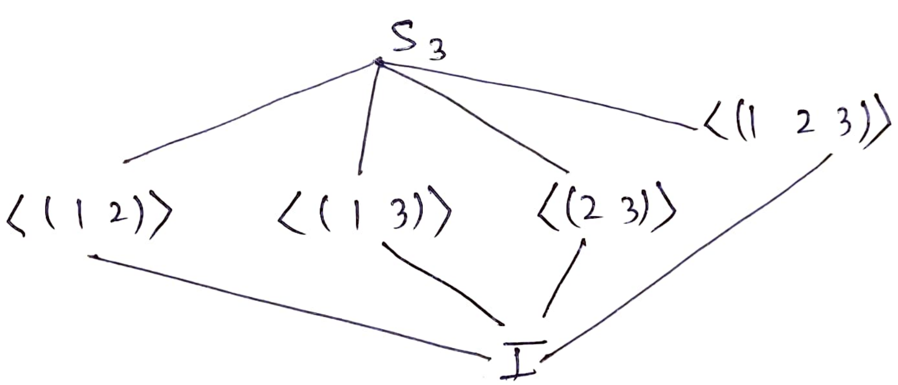
$$S_3 = \{ I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$$

$\langle (1,2) \rangle = \{ (1\ 2), I \}$

$\langle (1,3) \rangle = \{ (1\ 3), I \}$

$\langle (2\ 3) \rangle = \{ (2\ 3), I \}$

$\langle (1\ 2\ 3) \rangle = \{ (1\ 2\ 3), (1\ 3\ 2), I \}$



(4) The lattices of subgroups of $Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$

subgroups of Q_8 are: $\langle i \rangle, \langle j \rangle, \langle k \rangle, \langle -1 \rangle, \langle 1 \rangle$