Cyclic Groups

A cyclic group is a group generated by powers of an element *a* in the group. In order to understand this definition we must first explain what we mean by the power of an element.

As a concrete example let us consider the group

$$\mathbb{Z}_6 = \left(\{0,1,2,3,4,5\}, +\left(\mathrm{mod}\,6\right)\right)$$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Powers of the element 1 are defined by

$1^1 = 1$
$1^2 = 1 + 1 = 2$
$1^3 = 1 + 1 + 1 = 3$
$1^4 = 1 + 1 + 1 + 1 = 4$
$1^5 = 1 + 1 + 1 + 1 + 1 = 5$
$1^6 = 1 + 1 + 1 + 1 + 1 + 1 = 6$

In terms of the group structure (G, 0) *n*th power of the element $a \in G$ is the element

$$a^n = a \circ a \circ \ldots\ldots\ldots\ldots \circ a$$

where the composition is taken *n* times

This example demonstrates that $\mathbb{Z}_6$ is some power of 1.

$1^1 = 1$
$1^2 = 2$
$1^3 = 3$
$1^4 = 4$
$1^5 = 5$
$1^6 = 0$

To the definition of the power of an element $a \in G$, we add

$a^0 = e$, the identity element of G

a^{-1} is the inverse of element a.

The set of all powers generated by an element $a \in G$ is denoted by $\langle a \rangle$. It is the set

$$\langle a \rangle = \left(...a^{-3}, a^{-2}, a^{-1}, e, a, a^2.a^3, ...\right)$$
$$= \left\{a^r \,|r \in \mathbb{Z}\right\}$$

Thus

$\mathbb{Z}_6 \cong \langle 1 \rangle$

The powers of each element of a group *G* generates a cyclic subgroup of *G*.

For example, for $\mathbb{Z}_6$, consider the powers of 2.

$2^1 = 2$
$2^2 = 4$
$2^3 = 0$

Thus $\langle 2 \rangle = \{2, 4, 0\}$

Likewise

$3^1 = 3$
$3^2 = 0$

Thus $\langle 3 \rangle = \{3, 0\}$

Thus $\langle 2 \rangle$, $\langle 3 \rangle$ are distinct, proper cyclic subgroups of the group $\mathbb{Z}_6$

As the above examples indicate the symbol $\mathbb{Z}_n$ is often used to signify the cyclic group of order *n*. An alternative notation of the same cyclic group is C_n.

The order of a group is the number of elements in the group. The order of G is designated by the symbol

$|\mathrm{G}|$

For example $|\mathbb{Z}_6| = 6$

The order of an element a of a group G is the number of elements in the cyclic subgroup $\langle a \rangle$.

For $\mathbb{Z}_6$

$|\langle 2 \rangle| = 3$ and $|\langle 3 \rangle| = 2$

The order of $\langle a \rangle = s$. This means that

$a^s = e$ and that there does not exist an integer $k < s$ such that $a^k = e$.

So if G is a cyclic group of order s, then it follows from the definition of a cyclic group that there exists some element $a \in S$ such that $\langle a \rangle = S$ - the element a generates the set S under the group operation. A group is cyclic if there exists at least one element that generates the whole group, whose order is equal to the order of the group.

With these definitions and observations, further properties of cyclic groups can be explored, as in the following example.

Example

The set of all powers generated by an element $a \in G$ is denoted by $\langle a \rangle$.
It is the set

$$\langle a \rangle = \left(...a^{-3}, a^{-2}, a^{-1}, e, a, a^2.a^3, ...\right)$$
$$= \left\{ a^r \,|\, r \in \mathbb{Z} \right\}$$

The order of $\langle a \rangle = s$. This means that

$a^s = e$ and that there does not exist an integer $k < s$ such that $a^k = e$.

Show that with this definition, no two elements of the set

$e,\ a,\ a^2,\ a^3,\ ....,\ a^{s-1}$

can be identical

Solution

Suppose that there were two elements that were identical; then let
a^k and a^l be these two elements, where $k < l < s$
So we have
$a^k = a^l$

Multiplying on both sides by the inverse of a^k
$a^k a^{-k} = a^l a^{-k}$
$a^0 = a^{l-k}$
$a^{l-k} = e$

Hence, there is a positive integer, $l - k < s$ such that
$a^{l-k} = e$
Hence the order of the cylic group is $l - k < s$
This contradicts the supposition that the order of the group is s.
Hence there cannot be two elements such that $a^k = a^l$ where $k < l < s$
Hence, no two elements of the set

$e,\ a,\ a^2,\ a^3, ..., a^{s-1}$

can be identical, as required.