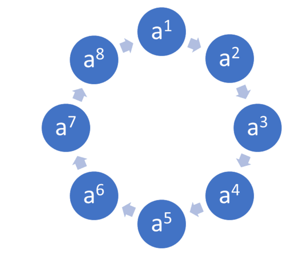
Generators of Cyclic Groups

Emily McDonagh, Lisa Murphy and Sarah Egan

17426532 , 17442254 , 17371311



Definitions

A group G is said to be *'cyclic'* if it can be generated by at least one element in the group. A cyclic group is denoted by Cn.
If a group is cyclic the element or elements that can generate the whole group are referred to as generators of the group. This generator is denoted by the brackets <>.

Explanation: Let G be a group under the binary operation of addition.
Now, let $x\epsilon G$.
The group generated by <x> is the smallest subgroup of G containing x. i.e. G=<x>

Notes

- All cyclic groups are abelian.
- There are two types of cyclic groups : Infinite and finite.
- The trivial group consisting of the identity element denoted (e) is arbitrarily cyclic.
- It is possible for non-cyclic groups to contain cyclic subgroups.

Infinite Cyclic Groups

Example:

$(\mathbb{Z}, +)$ Integers under the binary operation of addition. As the binary operation is addition the generator will take the form of

$$< a >= na | n \in \mathbb{Z}$$

This is the only example of an **infinite cyclic group**.
It has only 2 generators :

$$< 1 > \text{ and } < -1 >$$

For any element <x> to be a generator of a group it must be able to generate:

1. the identity element. (0)
2. the inverse of itself.
3. every multiple of the element.

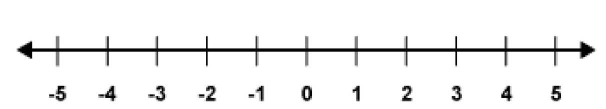


Fig. 1: Infinite number-line

Finite Cyclic Groups

Example:

$(\mathbb{Z}|n\mathbb{Z}, +)$ Integers under addition modulo n.

This is a finite group of n elements where n $\epsilon\mathbb{N}$
Elements of $\mathbb{Z}_n = (0, 1, 2, ..., n-1)$
Applying the group operation to these elements will generate:

$$(.. -2, -1, 0, 1, 2, ..., n-1, n, n+1, n+2..)$$
$$n \equiv 0mod(n)$$
$$n+1 \equiv 1mod(n)$$
$$n+2 \equiv 2mod(n)$$
$$. \; . \; . \; . \; .$$
$$-2 \equiv n-2mod(n)$$
$$-1 \equiv n-1mod(n)$$

The group generated by $< 1 >$ cycles through the numbers (0 - n-1) repeatedly therefore it is referred to as a *'cyclic'* group.

Notes

- Depending on the value of n, generators other than <1> will be present.

Examples

- C_6 (Integers under addition modulo 6)
  The elements 1 and 5 generate C_6 , since:

$$1 = 1 \qquad 5 = 5$$
$$1+1 = 2 \qquad 5+5 = 4\text{mod } 6$$
$$1+1+1 = 3 \qquad 5+5+5 = 3\text{mod } 6$$
$$1+1+1+1 = 4 \qquad 5+5+5+5 = 2\text{mod } 6$$
$$1+1+1+1+1 = 5 \qquad 5+5+5+5+5 = 1\text{mod } 6$$
$$1+1+1+1+1+1 = 0 \qquad 5+5+5+5+5+5 = 0\text{mod } 6$$

  You can see that the two elements <1> and <5> each individually generate all elements of C_6. These are the only two generators.

- C_8(Integers under addition modulo 8)
  The cyclic group C_8 has 4 generators. These are:

  <1>, <3>, <5> and <7>

  Each of these elements under repeated addition upon themselves will generate to whole group:

$$C_8 = (0,1,2,3,4,5,6,7)$$

Examples ctd.

Observe the cyclic structure of C_8 below:

C_8

	$I.D._c$	1	2	3	4	5	6	7
$I.D._c$	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Fig. 2: Infinite number-line

Non- Example

D5 is dihedral group that is a non-example.
Dihedral groups are groups of symmetries of a regular polygon. Such symmetries can be seen in a regular pentagon.
D5 is not abelian and therefore is not cyclic as all cyclic groups are abelian.

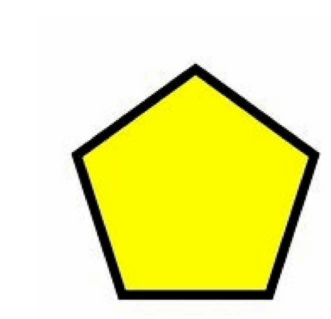


Fig. 3: D5- a non example of a cyclic group

Number of Generators of a group of Order n

All the generators of a finite group C_n are ones that are relatively prime to n, i.e. have a **gdc** of 1 with n.
General Rule: Two generators of any cyclic group of order n will always be:

$$< 1 > \text{ and } < n-1 >$$

Looking at C8 we have previously stated that the gererators are: 3,5,7,1. The other elements (0,2,4,6) are not co-prime to n=8 therefore will not generate the entire group. i.e.

$$< 0 >= (0)$$
$$< 2 >= (2, 4, 6, 0)$$
$$< 4 >= (4, 0)$$
$$< 6 >= (6, 4, 2)$$