Cyclic Groups and their Generators

Dean Gavagan

† Department of Mathematics, National University of Ireland Galway.

Cyclic Groups and their Properties

A *cyclic group* is a group, all of whose elements are *generated*, by particular element: $x \in G$. We can expand on this and say that G is no more than the set containing all those elements which can be generated from x. When we say x is a *generator*, we mean, simply, that it is a primitive or base element of the set.
For a *cyclic group*, G, we then write: $G =< x >$ and say: x *generates* G.

Properties of Cyclic Groups

- Every cyclic group is abelian. Its group operation is commutative, meaning: $xy = yx \; \forall \; x, y \in G$.
- An important fact arises out of this abelian property: each of conjugacy class of G, consists of only one element. This is why the order of a cyclic group is equal to the order of its generator; since a cyclic group of order n, has n, conjugacy classes.
- A subgroup of a cyclic group is a cyclic group, however cyclic subgroups can appear for non-cyclic groups also.
- If G is a finite finite group, then the order of any elent of G divides G.
- Any two cyclic groups of the same order, whether *finite* or *infinite*, are *isomorphic*.

Finite Cyclic Groups and their Structure

Since a group G is called cyclic if:

$$\exists \; x \in G$$

such that $< x >= G$ and that any such x is called a generator of G.

$$\Rightarrow G =< x >$$

is a cyclic group of order $n < \infty$, then

$$G = e, x, ..., x^n 1$$

,all elements $e, x, ..., x^n 1$ are distinct, and so:

$$x^n = e$$

.

Let $G =< x >$ be a finite cyclic group of order n. The following must hold:

- Every subgroup of G is cyclic and is equal to $< x^d >$. Here we have $d \geq 0$ and $d|n$
- If a and b are positive divisors of n and $a \neq b$, then $< x^a > \neq < x^b >$
- If $k \in \mathbb{Z}$, then x^k is a generator of $G \leftrightarrow k$ and n are coprime.
- For any $k \in \mathbb{Z}$ we have $< x^k >=< x^d >$ where $d = \gcd(n, k)$
- For any $k \in \mathbb{Z}$ we have $o(x^k) = \frac{n}{gcd(n,k)}$

Ultimately, a group is both finite and cyclic if it is isomorphic to the group of integers modulo n for some positive integer n.

Infinite Cyclic Groups

There is only one candidate to exemplify an infinite cyclic group; that is $G = (\mathbb{Z}, +)$, in which case $x =< 1 >, < -1 >$ are the generators. For example; if n is a positive integer, $\mathbb{Z}n$ is a cyclic group of order n generated by 1. We say here, that 1, generates: Z_7, since

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

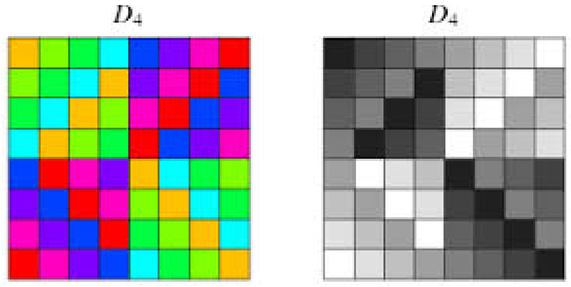
$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of ± 1.
More precisely it is the only infinte cyclic group up to isomorphism.

A subsequent lemma of this is that:

$$\forall x \in G, x \neq e \mid \forall m, n \in \mathbb{Z} : m \neq nx m \neq xn$$

Here, e is the identity element of G. That is, such that all the powers of x are distinct.

Examples of Cyclic and Non-cyclic Groups

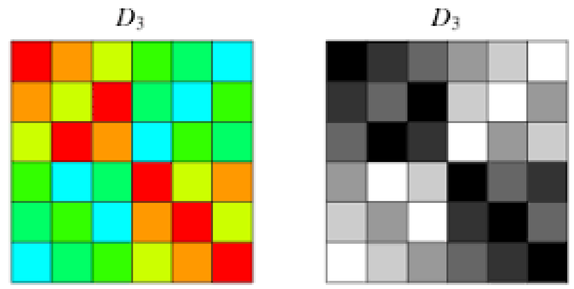


Above are representative group tables, illustrating the inherent pictographic nature of cyclic groups.

In the first figure we have the cyclic dihedral group D_4 dihedral group. In fact, all D_2n dihedral groups are cyclic.

The cycle graph of D_4 as shown, has cycle index given by:

$$\mathbb{Z}(D_4) = \frac{1}{8}x_1^4 + \frac{1}{4}x_2x_1^2 + \frac{3}{8}x_2^2 + \frac{1}{4}x_4.$$



Above are the dihedral groups D_3. It represents an example of a group that is not cyclic in nature and so; no singular element can ever be met with luck in producing all other elements of the group.

The cycle graph of D_3 is shown above. D_3 has cycle index given by:

$$\mathbb{Z}(D_3) = \frac{1}{6}x_1^3 + \frac{1}{2}x_2x_1 + \frac{1}{3}x_3.$$

How Such Groups are Generated

A cyclic group can have more than one generator.
Notice how 3 generates $\mathbb{Z}_{\not 6}$

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

The group can also be written using multiplicative notation:
Z(7) = {1, a, a2, a3, a4, a5, a6} . In this form, a is a generator of $\mathbb{Z}_{\not 6}$. It turns out that in $\mathbb{Z}(\not 6) = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group. On the other hand, in $\mathbb{Z}(\not 6) = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate.