Lecture 6

We start by defining cyclic groups.

Definition A group G is cyclic if $\exists$ an element $a \in G$ such that $\langle a \rangle = G$.
Such an a is called a generator of G.
The examples $\mathbb{Z}$ and $\mathbb{Z}_6$ show that cyclic groups can be both infinite and finite.
However all the examples which we saw were abelian. This is always true :-

Proposition Cyclic groups are abelian.

Proof: Left as an easy exercise. $\blacksquare$

Now that we have learnt about subgroups and just encountered a new concept of cyclic groups, Our first instinct should be to understand the subgroups of a cyclic group. This is recurring theme in mathematics; once you learn a new topic, try to relate it to previously learned topics.

So let's go back to our set of examples of cyclic groups :-

1) $(\mathbb{Z}, +)$. We saw that the set of even integers $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. But then

$2\mathbb{Z} = \langle 2 \rangle$ and so it is a cyclic group.

Let's try $3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$ which are multiples of 3. This again is a subgroup and is a cyclic group with 3 as a generator. In fact, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, $\forall\, n \in \mathbb{Z}$ and $n\mathbb{Z} = \langle n \rangle$, so is a cyclic group.

2) Let's look at $(\mathbb{Z}_6, +)$ which is a cyclic group generated by $\langle 1 \rangle$. Check that $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$ and again $\{0,2,4\} = \langle 2 \rangle$, so it is a cyclic group.

<u>Exercise</u> :- Try to formulate a result (or Theorem) based on the observations of the above examples.

The observations above hints that a subgroup of a cyclic group is itself cyclic. This is precisely the next

<u>Theorem</u> :- Every subgroup of a cyclic group is cyclic.

<u>Proof</u> :- Suppose G is a cyclic group with a

a generator a, so $G = \langle a \rangle$. Let H be a subgroup of G. We want to find an element $b \in H$ such that $H = \langle b \rangle$.

First of all if $H = \{e\}$ or $H = G$ then the result is true, so suppose H is a proper subgroup of G. Pick any element $c \in H$, $c \neq e$. Then $c \in G$ as well and so $c = a^k$ for some $k \neq 0$, $k \in \mathbb{Z}$. Since H is a subgroup, so $c^{-1} = a^{-k} \in H$. So we know that H contains a positive power of a. But we want to find an element, that will generate all other elements, so intuitively it seems to choose a^m such that m is the smallest positive integer with $a^m \in H$ (why can we do this?)

Claim :- $H = \langle a^m \rangle$

Proof of the claim :- Let $x \in H$ be arbitrary.

We want to show that $x = (a^m)^n$ for some $n \in \mathbb{Z}$. Since $y \in G$ as well so $y = a^r$ for some $r \neq 0$. By division algorithm

$$r = nm + \beta \quad \text{with} \quad 0 \leq \beta < m.$$

So,
$$y = a^r = a^{nm+\beta}$$
$$= a^{nm} \cdot a^\beta = (a^m)^n \cdot a^\beta$$

$$\Rightarrow \quad a^\beta = (a^m)^{-n} \cdot y$$

But $a^m \in H \Rightarrow (a^m)^{-1} \in H$ and $y \in H \Rightarrow$ $(a^m)^{-n} \cdot y \in H \Rightarrow a^\beta \in H$. But m was chosen to be the smallest power of a such that $a^m \in H$, and $\beta < m \Rightarrow \beta = 0$.

So $y = (a^m)^n$. So any arbitrary $y \in H$ is a power of a^m and hence $H = \langle a^m \rangle$.

$\blacksquare$

Remark :- Note that the proof of the Theorem is telling us a lot more! We not only know that any $H \leq G$ is cyclic but we also know a generator of H. How? We know the generator of $G = \langle a \rangle$. Simply find the smallest, or the first power of a which is in H and that will be the generator.

e.g. in the case of $2\mathbb{Z} \leq \mathbb{Z}$, a generator of $\mathbb{Z}$ is 1. Then 2 is the smallest power of 1 such that $1+1 = 2 \in 2\mathbb{Z}$ and so $\langle 2 \rangle = 2\mathbb{Z}$.