Lecture 8

In the last lecture, we saw that the order of a subgroup of a cyclic group divides the order of the group. But is the converse true, i.e., for every divisor, say k of the order of the group, does $\exists$ a subgroup of the group of order k?

The following theorem answers that. It is a classification theorem, i.e., it classifies all the subgroups of a cyclic group.

Theorem Fundamental Theorem of Cyclic Groups

Let G be a cyclic group of order n and let $G = \langle a \rangle$. Then

(1) Every subgroup of G is cyclic.
(2) The order of any subgroup of G divides n.
(3) For every positive divisor k of n, G has exactly one subgroup of order k and it is $\langle a^{\frac{n}{k}} \rangle$.

Proof:- We have already proved parts (1) and (2) in

Lec. 6 and 7 respectively. So let's prove (3). Let k be any positive divisor of n. We will show that $\langle a^{\frac{n}{k}} \rangle$ is the only subgroup of order k. First of all, $\langle a^{\frac{n}{k}} \rangle$ is a subgroup.

In order to find $|\langle a^{n/k} \rangle|$, recall from Lec. 7 that order of such a subroup is $\dfrac{n}{\gcd(n, \frac{n}{k})}$. Now $\gcd(n, \frac{n}{k}) = \frac{n}{k} \Rightarrow$

$|\langle a^{n/k} \rangle| = n/_{n/k} = k$, so it is indeed of order k.

Now we want to prove that this is the only one of order k. Suppose $H \leq G$ and $|H| = k$. Then by (1) H must be cyclic and so $H = \langle a^m \rangle$ for some $m \in \mathbb{Z}_+$. From part (2) we know that $m \mid n$. Now $|H| = k$ and also, $|H| = |\langle a^m \rangle| = \dfrac{n}{\gcd(m,n)}$. But $\gcd(m,n) = m$.

So, $k = \dfrac{n}{m} \Rightarrow m = \dfrac{n}{k}$ and hence $H = \langle a^{\frac{n}{k}} \rangle$.

The proof of the theorem is complete. $\boxed{////}$

Let's try to see what the theorem is saying by an example.

<u>Example</u> :- Suppose we have a cyclic group of order 12, i.e., $G = \langle a \rangle$, $\text{ord}(a) = |G| = 12$.
So the theorem is telling us that all the subgroups of G are themselves cyclic [Part (1)].
We know apriori what are the possibilities for the order of the subgroups (must divide 12) hence can be 1, 2, 3, 4, 6, 12 [Part (2)] and finally Part (3) is telling us that the subgroups of the aforementioned orders do occur and we can describe their generators too!

Order	Subgroup
1	$\{e\}$
2	$\langle a^{\frac{12}{2}} \rangle = \langle a^6 \rangle$
3	$\langle a^4 \rangle$
4	$\langle a^3 \rangle$
6	$\langle a^2 \rangle$
12	$\langle a \rangle = G$

Note that the subgroup of order 3 $\langle a^4 \rangle$ is also a subgroup of order 6 $\langle a^2 \rangle$.

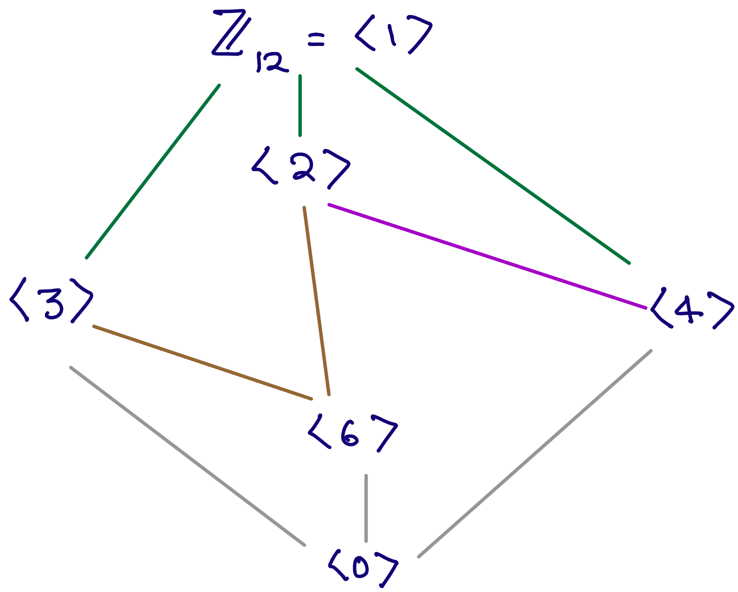
<u>Definition</u> A subgroup lattice is an illustration which describes relationships among various subgroups of a group.

It is a diagram that includes all the subgroups of a group and connects a subgroup H, say, at one level to a subgroup, K, say at a higher level if and only if H is a proper subgroup of K. (Recall the definition of a proper subgroup).

<u>Remark</u> The notion of a subgroup lattice makes sense for any group and not just cyclic groups.

So, first write down all the subgroups of a group G with G on the top and then add a line between a subgroup at a higher level and a subgroup at a lower level if and only if the latter is a proper subgroup of the former.

e.g. let's draw the subgroup lattice of $\mathbb{Z}_{12}$, which is cyclic of order 12, $\mathbb{Z}_{12} = \langle 1 \rangle$ and hence from the above example, we know all its subgroups.



looks pretty, ain't it?

We saw that the order of a subgroup of a cyclic group divides the order of the group and made a remark in the last lecture that it is a more general phenomenon, in fact a theorem due to Lagrange. In the next lecture, we'll see what the theorem is and how to prove it using the notion of cosets.