Lecture 20

We'll start by classifying all groups upto isomorphism upto order 7.

What does groups upto isomorphism means?

We'll consider two groups G and G' as "same" if $G \cong G'$. So, classifying groups of order, say n, upto isomorphism means that we want to make a list of all groups of order n such that no two groups on the list are isomorphic and any other group of order n must be isomorphic to one of the groups on our list.

This will make much more sense when we make the list below.

Let's start with order 1. There is only one group of order 1 ; $\{e\}$. So the list is complete for order 1.

Order 2 Since 2 is a prime $\Rightarrow$ any group G, $|G| = 2$ must be cyclic. Now any cyclic group of order $n \cong \mathbb{Z}_n$ $\Rightarrow$ ie this case $G \cong \mathbb{Z}_2$.

So the only group of order 2, upto isomorphism is $\mathbb{Z}_2$.

By the similar reasoning the list of groups, upto isomorphism for

Order 3	$\mathbb{Z}_3$
order 5	$\mathbb{Z}_5$
order 7	$\mathbb{Z}_7$

Order 4 Let G be a group of order 4. By Lagrange's Theorem, if $a \in G, a \neq e$ then $ord(a) = 2$ or 4. If $ord(a) = 4 \Rightarrow G$ is cyclic.

If G is not cyclic then $\forall\, a \in G$, $ord(a) = 2$ $\Rightarrow a^2 = e \Rightarrow G$ is abelian.

So first of all, any group G of order 4 is abelian.

Also, the above argument shows that either G is cyclic, in which case $G \cong \mathbb{Z}_4$, or every element of G has order 2 $\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

We know from Assignment 3, $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus, all the groups of order 4, upto isomorphism, are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

So now let's focus on groups of order 6.

We already know examples of both abelian and nonabelian groups of order 6 : $\mathbb{Z}_6$ for abelian and D_3 for nonabelian. We know S_3 too but as seen in assignment 2 that $S_3 \cong D_3$, so on the list S_3 will be considered same as D_3.

So now we divide our problem in two cases:-

<u>Case 1</u> G is abelian.

If $a \in G$, $a \neq e$ $\Rightarrow$ ord $(a) = 2, 3$ or 6.

If ord $(a) = 6$ $\Rightarrow$ G is cyclic and hence $G \cong \mathbb{Z}_6$.

Now if we do not know if G has an element of order 6, then by Cauchy's Theorem, since $2 \mid 6$, $\exists$ $a \in G$ s.t. ord $(a) = 2$.

Again by Cauchy's theorem, $\exists$ $b \in G$ s.t. ord$(b) = 3$

Now, G is abelian $\Rightarrow$ $ab = ba$ and $\gcd(2,3) = 1$

so from a question from Q.2 (a) on Assignment

2, $\text{ord}(ab) = 6 \Rightarrow G$ is cyclic.

So if G is an abelian group of order 6 then it must be cyclic and hence $\cong \mathbb{Z}_6$.

<u>Case 2</u> G is nonabelian.

If G is nonabelian then G can't have an element of order 6. Then for $a \in G$, $a \neq e$, $\text{ord}(a) = 2$ or $\text{ord}(a) = 3$. If $\forall\, a \in G$, $\text{ord}(a) = 2 \Rightarrow G$ is abelian, so $\exists$ some $a \in G$ with $\text{ord}(a) = 3$. Now since elements of order come in pair and $\text{ord}(e) = 3 \Rightarrow$ not every element can have order 3 because $|G| = 6$. So $\exists\, b \in G$ with $\text{ord}(b) = 2$.

So $G = \{e, a, a^2, b, ab, ab^2\}$

Now $ba \in G$, so it must be one of the elements listed above. Let's see what would it be.

If $ba = e \Rightarrow a = b^{-1} = b$, which is not possible as $\mathrm{ord}(a) = 3$ and $\mathrm{ord}(b) = 2$. ✗

If $ba = a \Rightarrow b = e$, not possible ✗

If $ba = a^2 \Rightarrow b = a$, not possible ✗

If $ba = b \Rightarrow a = e$, not possible ✗

If $ba = ab$, then again by Q.2(a) on Assignment 2, $\mathrm{ord}(ab) = 6 \Rightarrow G$ is cyclic, not possible. ✗

So the only possibility is that $ab^2 = ba$. But this is precisely what happens in D_3!, i.e., if we send $a \longmapsto R_{120}$ and b to any of the flip, then $G \cong D_3$.

Hence if G is nonabelian, $|G| = 6$ then $G \cong D_3$.

Thus, upto isomorphism, there are two groups of order 6 :- $\mathbb{Z}_6$ and D_3.

This is how we classify groups of a certain order. We might need more tools than those required in the previous discussion and this is what we plan to do.

So, let's see some properties of a homomorphism.

<u>Proposition 1</u> Let $\varphi : G \to \bar{G}$ be a homomorphism. Then

1) $\varphi(e) = \bar{e}$, $\bar{e}$ is ~~the~~ identity of $\bar{G}$.
2) For $a \in G$, $\varphi(a^{-1}) = [\varphi(a)]^{-1}$.
3) $\forall\, n \in \mathbb{Z}$, $\varphi(a^n) = [\varphi(a)]^n$.
4) If $\mathrm{ord}(a)$ is finite then $\mathrm{ord}(\varphi(a)) \mid \mathrm{ord}(a)$

5) Let $H \leq G$. Then $\varphi(H) = \{\varphi(h) \mid h \in H\} \leq \overline{G}$.

6) If H is cyclic then $\varphi(H)$ is cyclic.

7) If H is abelian then $\varphi(H)$ is abelian.

8) If $H \triangleleft G$ then $\varphi(H) \triangleleft \overline{G}$.

9) If $|H| = n$, then $|\varphi(H)| \mid n$.

10) If $\overline{K} \leq \overline{G}$, then $\varphi^{-1}(\overline{K}) = \{k \in G \mid \varphi(k) \in \overline{K}\}$ is a subgroup of G.

11) If $\overline{K} \triangleleft \overline{G}$, then $\varphi^{-1}(\overline{K}) \triangleleft G$.

<u>Proof</u> The proofs of 1), 2) and 3) are same as that for the properties of an isomorphism.

4) follows from 3) as if $\operatorname{ord}(a) = n \Rightarrow$

$a^n = e \Rightarrow \varphi(a^n) = [\varphi(a)]^n = \varphi(e) = \overline{e}$

$\Rightarrow \operatorname{ord}(\varphi(a)) \mid \operatorname{ord}(a)$.

Note that in case of an isomorphism, $\operatorname{ord}(a) =$

ord($\varphi(a)$). But for a homomorphism we can only say that ord $(\varphi(a)) \mid$ ord (a).

e.g. consider $\varphi: \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ given by

$\varphi(a) = 10a \bmod 30$.

One can check that φ is a homomorphism.

now, for $1 \in \mathbb{Z}_{12}$, ord$(1) = 12$. $\varphi(1) = 10$ and ord(10) $= 3$ in $\mathbb{Z}_{30}$. So ord$(\varphi(1)) \neq$ ord(1) and ord$(\varphi(1)) \mid$ ord(1).

The proofs of rest of the statements are left as an easy exercise. [Some of them will be on Assignment 4].

Recall that if $\varphi: G \to \overline{G}$ is a homomorphism then

$$\mathrm{Ker}(\varphi) = \{ g \in G \mid \varphi(g) = \overline{e} \}$$

We know that $\mathrm{Ker}(\varphi) \leq G$.

<u>Proposition 2</u> $Ker(\varphi) \triangleleft G$.

<u>Proof</u> First of all we'll have to prove that $Ker(\varphi) \leq G$. Note that $\varphi(e) = \bar{e} \Rightarrow e \in Ker(\varphi)$.

So $Ker(\varphi) \neq \phi$. We'll use the subgroup test.

Let $a \in Ker(\varphi)$, $b \in Ker(\varphi)$ $\Rightarrow$ $\varphi(a) = \bar{e}$, $\varphi(b) = \bar{e}$

We want to show that $ab^{-1} \in Ker(\varphi)$.

Consider $\varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b^{-1})$ [as φ is a homomo-rphism]

$= \varphi(a)\varphi(b)^{-1}$ [from 2) of Prop. 1]

$= \bar{e} \cdot \bar{e}^{-1} = \bar{e}$

So $ab^{-1} \in Ker(\varphi) \Rightarrow Ker(\varphi) \leq G$.

Now, we'll use the normal subgroup test.

Let $g \in G$ and $a \in Ker(\varphi)$. We want to check if $gag^{-1} \in Ker(\varphi)$. Then

$\varphi(gag^{-1}) = \varphi(g) \cdot \varphi(a) \cdot \varphi(g)^{-1}$

$= \varphi(g)\cdot \bar{e} \cdot \varphi(g)^{-1} = \varphi(g)\cdot \varphi(g)^{-1} = \bar{e}$

So, $gag^{-1} \in \ker(\varphi)$ and $\ker(\varphi) \trianglelefteq G$.

$\boxed{\text{Pr.}}$

Let's end this lecture by counting the # of homomorphisms from $\mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{30}$. Note that there is no isomorphism b/w $\mathbb{Z}_{12}$ and $\mathbb{Z}_{30}$ as they have different orders.

So suppose $\varphi : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{30}$ is a homomorphism. Then we know everything about φ by looking at $\varphi(1)$.

Now $1 \in \mathbb{Z}_{12}$ has order 12. From 4) Prop. 1, we know that $\text{ord}(\varphi(1)) \mid 12$

Also, $\varphi(1) \in \mathbb{Z}_{30} \Rightarrow$ by Lagrange's theorem

$$\text{ord}(\varphi(1)) \mid 30 \quad \text{— } ②$$

So from ① and ② the choices for order of $\varphi(1)$ and hence for $\varphi(1)$ are

Order of $\varphi(1)$	$\varphi(1)$
1	0
2	15
3	10 or 20
6	5 or 25

Thus there are 6 choices of $\varphi(1)$ and one can check that each one of them indeed gives a homomorphism.

e.g. if $\varphi: \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ is given by

$\varphi(1) = 5$ then for $a \in \mathbb{Z}_{12}$

$$\varphi(a) = \varphi(\underbrace{1+1+\cdots+1}_{a\text{-times}}) = \underbrace{\varphi(1)+\cdots+\varphi(1)}_{a\text{-times}}$$

$$= 5a \bmod 30$$

$$\varphi(b) = 5b \bmod 30 \quad , b \in \mathbb{Z}_{12}$$

and
$$\varphi(a+b) = 5(a+b) \bmod 30$$
$$= 5a+5b \bmod 30$$

$$= 5a \bmod 30 + 5b \bmod 30$$

$$= \varphi(a) + \varphi(b)$$

So φ is a homomorphism. Thus

$$\#\{\text{homomorphism } \varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}\} = 6.$$