Lecture 19

Let's start by calculating $\mathrm{Inn}(D_4)$.

$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

So we want to find φ_g for $g \in D_4$.

Recall that the inner automorphism induced by $a \in G$ is defined as

$$\varphi_a : G \longrightarrow G, \quad \varphi_a(g) = a g a^{-1}$$

Note that, if $a \in Z(G)$, then

$$\varphi_a(g) = a g a^{-1} = g a a^{-1} = g \quad (\text{as } ag = ga)$$

So $\varphi_a = I$ if $a \in Z(G)$

$\therefore \quad Z(D_4) = \{R_0, R_{180}\} \Rightarrow \varphi_{R_0} = \varphi_{R_{180}} = I$

Consider $\varphi_{R_{270}}$. Since $R_{270} = R_{90} \cdot R_{180}$

So, $\varphi_{R_{270}}(g) = R_{270} \cdot g \cdot R_{270}^{-1}$, $g \in D_4$

$= (R_{90} \cdot R_{180}) \cdot g \cdot (R_{90} \cdot R_{180})^{-1}$

$= R_{90} (R_{180} \cdot g \cdot R_{180}^{-1}) R_{90}^{-1}$

$= R_{90} \cdot g \cdot R_{90}^{-1}$ $\quad$ (as $R_{180} \in Z(D_4)$)

$= \varphi_{R_{90}}(g)$

Since $g \in D_4$ was arbitrary $\Rightarrow$ $\varphi_{R_{270}} = \varphi_{R_{90}}$.

Now, $H = V \cdot R_{180}$ and $D = D' \cdot R_{180}$

so by the same reasoning as above, $\varphi_H = \varphi_V$

and $\varphi_D = \varphi_{D'}$.

Now $\varphi_{R_{90}} \neq I$ as $\varphi_{R_{90}}(H) = R_{90} \cdot H \cdot R_{90}^{-1}$

$= V$ so $\varphi_{R_{90}} \neq I$.

Also $\varphi_{R_{90}}(H) = V$ and $\varphi_H(V) = H \cdot V \cdot H^{-1}$
$= R_{270}$

$\Rightarrow \varphi_{R_{90}} \neq \varphi_H$.

Similarly, one can check that all of $\varphi_{R_{90}}, \varphi_H$ and φ_D are different $\Rightarrow$

$$\mathrm{Inn}(D_4) = \{ I, \varphi_{R_{90}}, \varphi_H, \varphi_D \}$$

Now, suppose $\varphi \in \mathrm{Aut}(\mathbb{Z}_n)$, i.e., $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ is an automorphism. Remember the following principle

Any homomorphism / isomorphism / automorphism of a cyclic group is determined by its action on a generator.

Since $\mathbb{Z}_n = \langle 1 \rangle$ so φ is completely determi-
-ned by $\varphi(1)$. Now $\varphi(1) \in \mathbb{Z}_n$ must also be a generator as φ is an isomorphism.

But we know all the generators of $\mathbb{Z}_n$!

$$\mathbb{Z}_n = \langle a \rangle \iff \gcd(a,n) = 1$$

So, $\varphi(1)$ must be coprime to n.

Thus, $\varphi(1) \in U(n)$.

So for any automorphism of $\mathbb{Z}_n$, we have an element of $U(n)$. The next theorem says that every element of $U(n)$ gives rise to an automorphism of $\mathbb{Z}_n$. In fact, $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$ as groups.

Theorem For $n \in \mathbb{N}$, $U(n) \cong \mathrm{Aut}(\mathbb{Z}_n)$.

Proof We'll explicitly give an isomorphism b/w $\mathrm{Aut}(\mathbb{Z}_n)$ and $U(n)$.

Define $F : Aut(\mathbb{Z}_n) \longrightarrow U(n)$ by

$$F(\varphi) = \varphi(1) \quad \forall \quad \varphi \in Aut(\mathbb{Z}_n)$$

<u>F is one-one</u>

Suppose, $F(\varphi) = F(\tau)$, $\varphi, \tau \in Aut(\mathbb{Z}_n)$

$\Rightarrow \quad \varphi(1) = \tau(1)$

But $\mathbb{Z}_n = \langle 1 \rangle \quad \Rightarrow \varphi(1) = \tau(1)$ gives that

$\varphi = \tau$. So F is one-one.

<u>F is onto</u>

Let $r \in U(n)$. We want to find an element $\varphi \in Aut(\mathbb{Z}_n)$ such that $F(\varphi) = r$.

Now we know that $T(\varphi) = \varphi(1)$, so we want $\varphi(1) = r$. So we define

$$\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \text{ by}$$

$$\varphi(s) = rs \mod n$$

Clearly $\varphi(1) = r$.

Check :- φ is an automorphism of $\mathbb{Z}_n$.

Also , $F(\varphi) = \varphi(1) = r$

$\Rightarrow$ F is onto.

<u>F is a homomorphism</u>

Let $\varphi, \tau \in Aut(\mathbb{Z}_n)$. Want to check

$$F(\varphi \circ \tau) = F(\varphi) \cdot F(\tau)$$

$$F(\varphi \circ \tau) = \varphi \circ \tau(1) \quad \text{(by definition)}$$

$$= \varphi(\tau(1))$$

$$= \varphi(\underbrace{1 + 1 + \cdots + 1}_{\tau(1)\text{-times}}) \quad \left(\text{as } \tau(1) \in \mathbb{Z}_n \text{ so we can write as sum of } 1\right)$$

$$= \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{\tau(1)\text{-times}} \quad \left(\text{as } \varphi \text{ is a homomorphism}\right)$$

$$= \varphi(1) \cdot \tau(1)$$

$$= F(\varphi) \cdot F(\tau)$$

So F is an isomorphism and hence

$\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$.

So we explicitly know what $\mathrm{Aut}(\mathbb{Z}_n)$ is.

In the next lecture, we'll use the tools so far to classify all groups upto isomorphism upto order 7.